National Security
Agency/Central Security Service

INFORMATION ASSURANCE DIRECTORATE

MOBILE ACCESS CAPABILITY PACKAGE

This Commercial Solutions for Classified (CSfC) Capability Package (CP) describes how to protect classified data (including Voice and Video) in Mobile Access Solutions transiting Wired Networks, Domestic Cellular Networks, and Trusted Wireless Networks to include Government Private Cellular Networks and Government Private Wi-Fi networks.

Version 1.0
April 2, 2015

Mobile Access Capability Package

CHANGE HISTORY

Title	Version	Date	Change Summary
Commercial Solutions for Classified (CSfC) Mobile Access Capability Package (CP) release for Public Comment	0.8	November 3, 2014	• Initial release of CSfC Mobile Access guidance for public comment. • Incorporates End User Device (EUD) Solution Designs from VPN version 3.0 CP. • Incorporates content from Mobile Security Guide version 2.3.
Commercial Solutions for Classified (CSfC) Mobile Access CP release for Public Comment	1.0	April 2, 2015	• Removed "Non-MDF Validated" EUD type • Removed EUD design utilizing two VPN Gateways • Removed option to utilize separate computing platform with VPN Client installed to provide Outer layer of encryption • Changed restrictions on control plane traffic • Added Tactical Solution Implementation Appendix • Added requirements for End User Device • Added requirements for Retransmission Device • Corrected language in requirement MA-CR-9 and made consistent with the MACP Compliance Matrix

TABLE OF CONTENTS

TABLE OF FIGURES

LIST OF TABLES

1 INTRODUCTION

The Commercial Solutions for Classified (CSfC) Program within the National Security Agency (NSA) Information Assurance Directorate (IAD) publishes Capability Packages (CPs) to provide configurations that empower IAD customers to implement secure solutions using independent, layered Commercial Off-the-Shelf (COTS) products. The CPs are product-neutral and describe system-level solution frameworks documenting security and configuration requirements for customers and/or Solution Integrators.

IAD delivers this CSfC Mobile Access (MA) CP to meet the demand for mobile data in transit solutions (including Voice and Video) using approved cryptographic algorithms and National Information Assurance Partnership (NIAP) evaluated components. These algorithms, known as Suite B algorithms, are used to protect classified data using layers of COTS products. MA CP Version 1.0 is the initial release to provide customer requirements for domestic and international voice, video, and data capabilities from a mobile End User Device. This CP builds on lessons learned from a CSfC Initial Solution that implemented secure voice and data capabilities using a set of Secure Sharing Suite (S3) algorithms, modes of operation, standards, and protocols. The CSfC Initial Solution leveraged lessons learned from customer pilot solutions utilized to protect classified data in mobile environments. The Initial Solution and Pilots included a layered use of COTS products for the protection of classified information.

The CSfC MA CP Version 1.0 builds on the End User Device (EUD) designs of the Virtual Private Network (VPN) CP Version 3.0 as well as the Mobility Security Guide Version 2.3. VPN Remote and Local EUD Designs which complied with the VPN CP Version 3.0, dated July 22, 2014, are expected to need only minor changes to comply with the VPN EUD Design of this CP.

2 PURPOSE OF THIS DOCUMENT

This CP provides high-level reference designs and corresponding configuration requirements that allow customers to select COTS products from the CSfC Components List available on the CSfC web page (http://www.nsa.gov/ia/programs/csfc_program), for their MA solution and then to properly configure those products to achieve a level of assurance sufficient for protecting classified data while in transit. As described in Section 12, customers must ensure that the components selected from the CSfC Components List will permit the necessary functionality for the selected capabilities. To successfully implement a solution based on this CP, all Threshold requirements, or the corresponding Objective requirements applicable to the selected capabilities, must be implemented, as described in Sections 11-13.

Customers who want to use this CP must register their solution with NSA. Additional information about the CSfC process is available on the CSfC web page (www.nsa.gov/ia/programs/csfc_program).

3 USE OF THIS DOCUMENT

This document, the CSfC Mobile Access CP Version 1.0, dated February 13, 2015, has been approved by the IAD Director and will be reviewed twice a year to ensure that the defined capabilities and other instructions still provide the security services and robustness required. Solutions designed according to this CP must be registered with NSA/IAD. Once registered, a signed IAD Approval Letter will be sent validating that the Mobile Access solution is registered as a CSfC solution validated to meet the requirements of the latest Mobile Access CP and is approved to protect classified information. Any solution designed according to this CP may be used for one year and must then be revalidated against the most recently published version of this CP.

Please provide comments on usability, applicability, and/or shortcomings to your NSA/IAD Client Advocate and the MA CP maintenance team at Mobile_Access@nsa.gov. MA CP solutions shall also comply with Committee on National Security System (CNSS) policies and instructions. Any conflicts identified between this CP and NSS or local policy should be provided to the MA CP Maintenance team.

The following Legal Disclaimer relates to the use of this CP:

This CP is provided "as is." Any express or implied warranties, including but not limited to, the implied warranties of merchantability and fitness for a particular purpose are disclaimed. In no event shall the United States Government be liable for any direct, indirect, incidental, special, exemplary or consequential damages (including, but not limited to, procurement of substitute goods or services, loss of use, data, or profits, or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of this CP, even if advised of the possibility of such damage.

The user of this CP agrees to hold harmless and indemnify the United States Government, its agents and employees from every claim or liability (whether in tort or in contract), including attorney's fees, court costs, and expenses, arising in direct consequence of Recipient's use of the item, including, but not limited to, claims or liabilities made for injury to or death of personnel of User or third parties, damage to or destruction of property of User or third parties, and infringement or other violations of intellectual property or technical data rights.

Nothing in this CP is intended to constitute an endorsement, explicit or implied, by the U.S. Government of any particular manufacturer's product or service.

4 DESCRIPTION OF THE MOBILE ACCESS SOLUTION

This CP describes a general MA solution to protect classified information as it travels across either an untrusted network or a network of a different classification level. The solution supports connecting EUDs to a classified network via two layers of encryption terminated on the EUD, provided that the EUD and the network operate at the same security level. The MA solution uses two nested, independent

tunnels to protect the confidentiality and integrity of data (including Voice and Video) as it transits the untrusted network. The MA Solution utilizes Internet Protocol Security (IPsec) as the outer tunnel and, depending on the Solution Design, IPsec or Transport Layer Security (TLS) as the Inner layer of protection.

Throughout this CP, the term "Inner Encryption Component" is used to refer generically to the component (device or software application) that terminates the Inner layer of encryption. An Inner Encryption Component can be a VPN Component or a TLS Component that is in the infrastructure or part of an EUD. The term "VPN Component" refers generically to both VPN Gateways and VPN Clients in situations where the differences between the two are unimportant. The Term "TLS Component" is used to denote a component that implements TLS between the infrastructure (TLS-Protected Server or Secure Real-time Transport Protocol (SRTP) Endpoint) and EUDs (TLS Client or SRTP Client) in accordance with this CP (see Sections 5.5 and 6 respectively). Finally, there are two EUD solution designs: VPN EUD and TLS EUD. The term "EUD" is used to refer generically to both designs where the differences between them are unimportant.

Table 1. Overview of Mobile Access CP Terminology

	VPN EUD	TLS EUD
Inner Encryption Component	IPsec provided by VPN Client	TLS or SRTP provided by TLS-Protected Server, SRTP Endpoint, TLS Client, **OR** SRTP Client
Outer Encryption Component	IPsec provided by VPN GW **OR** VPN Client	IPsec provided by VPN GW **OR** VPN Client

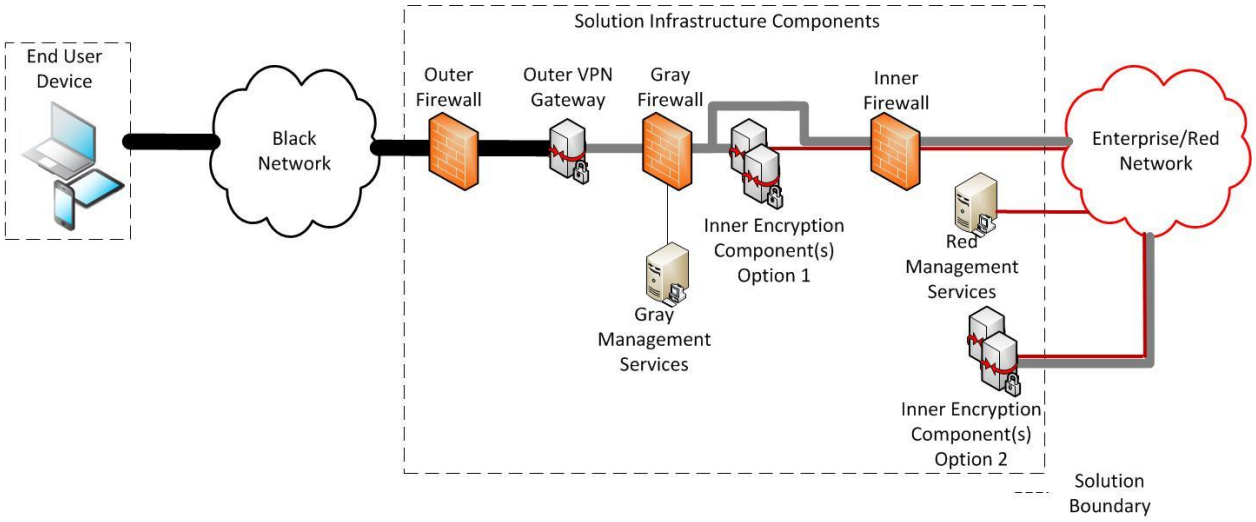

Figure 1. Two Layers of Encryption Protect Data across an Untrusted Network

As shown in Figure 1, before being sent across the untrusted network, classified data is encrypted twice: first by an Inner Encryption Component, and then by an Outer VPN Component. At the other end of the data flow, the received packet is correspondingly decrypted twice: first by an Outer VPN Component, and then by an Inner Encryption Component.

All Inner Encryption components, including those with only a connection to the Enterprise/Red network, are within the CSfC Solution Boundary. The MA CP allows the use of existing Classified Enterprise Network Encryption Components to provide the Inner layer of protection (e.g. Web Servers and Voice over Internet Protocol (VoIP) Desktop Phones), provided that the components are selected, configured, and tested in accordance with the requirements of this CP. When existing Classified Enterprise Network services are utilized as the Inner layer of encryption, they are within the MA Solution Boundary and reside on the internal side of the Inner firewall. There is no limit to the number of Inner Encryption Components permitted to terminate the Inner layer of encryption.

MA Solution components are managed using Red Management Services for Inner Encryption Components, and Gray Management Services for Outer Encryption Components. The Gray Management Services include an Administration Workstation to manage the Outer VPN Gateway, Gray firewall, a Security Information and Event Monitoring (SIEM) Component, and any additional components located between the Outer VPN Gateway and Inner Encryption Components. Gray Management Services may also manage a locally run Outer Certificate Authority (CA), Certificate Revocation List (CRL) Distribution Point (CDP), and/or Intrusion Detection System (IDS)/Intrusion Protection System (IPS). The Red Management Services include an Administration Workstation to manage the Inner Encryption Components, Inner firewall and other components within the Enterprise/Red Network. The Red Management Services may also manage a locally run Inner Certificate Authority (CA), and optionally, a Locally-run Outer CA. In addition, the MA CP allows customers to leverage an existing Enterprise Public Key Infrastructure (PKI) to issue Certificates to Outer VPN Components and Inner Encryption Components. To utilize an existing enterprise Root CA at least two separate subordinate CAs must be utilized: One to issue Certificates for Outer VPN Components and the other to issue Certificates for Inner Encryption Components.

The EUDs of the MA CP are form-factor agnostic. Typical MA CP EUDs include smart phones, tablets, and laptops. An MA CP EUD can be composed of multiple physical devices (for example a VPN Gateway and a Computing Device) all collectively referred to as the EUD. Although the CP allows flexibility in the selection of the EUD, the customer and Solution Integrator must ensure that EUDs meet all applicable requirements for the planned solution design. Section 4.2.1 describes in detail the differences between the VPN EUD and TLS EUD solution design options.

The MA CP instantiations are built using products from the CSfC Components List (see Section 12). Customers who are concerned that their desired products are not yet on the CSfC Components List are encouraged to contact the vendors to encourage them to sign a Memorandum of Agreement (MoA) with NSA and start the National Information Assurance Partnership (NIAP) evaluation process, which will

enable them to be listed on the CSfC Components List. Products listed on the CSfC Components List are not guaranteed to be interoperable with all other products on the Components List. Customers and Integrators should perform interoperability testing to ensure the components selected for their MA Solution are interoperable. If you need assistance obtaining vendor POC information, please email csfc_components@nsa.gov.

While CSfC encourages industry innovation, trustworthiness of the components is paramount. Customers and their integrators are advised that modifying a NIAP-evaluated component in a CSfC solution may invalidate its certification and trigger a revalidation process. To avoid delays, customers or integrators who feel it is necessary to modify a component should engage the component vendor and consult NIAP through their Assurance Continuity Process (see http://www.niap-ccves.org/Documents_and_Guidance/ccves/scheme-pub-6.pdf) to determine whether such a modification will affect the component's certification. In case of a modification to a component, NSA's CSfC Program Management Office requires a statement from NIAP that the modification does not alter the certification, or the security, of the component. Modifications which trigger the revalidation process include, but are not limited to the following: modifying the original equipment manufacturers' code (to include digitally signing the code) or not leveraging the baseline NIAP-evaluated configuration.

4.1 NETWORKS

This CP uses the following terminology to describe the various networks that comprise a MA solution and the types of traffic present on each. The terms Red, Gray, and Black refer to the level of protection applied to the data as described below.

4.1.1 ENTERPRISE/RED NETWORK

Red data consists of unencrypted classified data while Gray data consists of singly encrypted classified data. A Red network contains Red data and can contain Gray data. The Red network begins at the internal interface(s) of Inner Encryption Components located between the Gray firewall and Inner firewall. When a solution is implemented without an Inner Encryption Component between the Gray firewall and Inner firewall, then the Red network begins on the internal interface of the Inner firewall. EUDs access the Red network through the two layers of nested encryption described in this CP. For example, an Inner VPN Gateway, located between the Gray firewall and Inner firewall, terminates the Inner layer of IPsec encryption from a VPN EUD. Once a successful IPsec connection is established, the EUD is given access to classified services such as web, email, Virtual Desktop Infrastructure (VDI), voice, etc.

In some instances when the MA Infrastructure is designed to support TLS EUDs, the TLS-Protected Server or SRTP Endpoint, which terminates the Inner layer of encryption, will reside in the Enterprise/Red network on the internal side of the Inner firewall. In this design, the Inner firewall implements an Access Control List (ACL) which only permits traffic to reach TLS-Protected Servers and SRTP Endpoints which are within the CSfC Solution Boundary and terminate the Inner layer of

encryption. For example, an organization can choose to include Enterprise/Red network Web Servers within the CSfC Solution Boundary. The Web Servers would meet all applicable requirements of the MA CP and be configured to terminate an Inner layer of TLS traffic (Hypertext Transfer Protocol Secure (HTTPS)) originating from an EUD TLS Client (Web Browser). An alternative to this approach is to implement a TLS-Protected Server that includes both Gray and Red network interfaces located between the Gray firewall and Inner firewall. This TLS-Protected Server terminates the TLS connection from the EUD and proxies web data to the Enterprise/Red Web Servers which in this case would not be in the CSfC Solution Boundary. A similar situation exists for SRTP, by using a VoIP Gateway/Border Controller to terminate the SRTP traffic for an EUD, and relaying the data to the Enterprise/Red network. When a VoIP Gateway/Border Controller terminates the Inner layer of SRTP, Desktop Phones in the Enterprise/Red network are not included in the Solution Boundary.

The Enterprise/Red networks are under the control of the solution owner or a trusted third party. Enterprise/Red networks may only communicate with an EUD through the MA solution if both operate at the same security level.

4.1.2 GRAY NETWORK

Gray data is classified data that has been encrypted once. Gray networks are composed of Gray Data. Gray networks are under the physical and logical control of the solution owner or a trusted third party. Gray Data may extend into the Enterprise/Red network when enterprise TLS-Protected Servers (i.e. Web server) or SRTP Endpoints (i.e. VoIP Desktop Phone) terminate the Inner layer of encryption as described in Section 4.1.1. The Gray network is physically treated as a classified network even though all classified data is singly encrypted. If a solution owner's classification authority determines that data on a Gray Network is classified, perhaps by determining the Internet Protocol (IP) addresses are classified at some level; then, the MA solution described in this CP cannot be implemented, as it is not designed to provide two layers of protection for any classified information on the Gray Network.

Gray network components consist of the Solution Infrastructure Outer VPN Gateway, Gray firewall, and Gray Management Services. All Gray network components are physically protected at the same level as the Enterprise/Red network components of the Solution Infrastructure. Gray Management Services are physically connected to the Gray firewall and includes, at a minimum, an Administration Workstation. The MA CP requires the management of Gray Network components through the Gray Administration Workstation. As a result, neither Enterprise/Red nor Black administration workstations are permitted to manage the Outer VPN Gateway, Gray firewall, or Gray Management Services. Additionally, the Gray Administration Workstation is prohibited from managing Inner Encryption Components. These Inner Encryption Components must be managed from an Enterprise/Red Administration Workstation.

4.1.3 BLACK NETWORK

A Black network contains classified data that has been encrypted twice. The network connecting the Outer VPN Components together is a Black network. Black networks are not necessarily (and often will not be) under the control of the solution owner, and may be operated by an untrusted third party. The MA CP allows EUDs to operate over any Black network when used in conjunction with a Government-owned Retransmission Device (RD) or a physically separate VPN Gateway to establish the Outer IPsec Tunnel. A RD provides a connection to the MA solution infrastructure via any Black network and interfaces to the EUD using Wi-Fi or an Ethernet cable however, the CP does not permit the use of Ethernet over USB. Black networks include non-domestic cellular carrier networks, public Wi-Fi networks, wired connections (to the Internet for example), and any other wireless or wired networks.

The Government-owned RD is a category which includes Wi-Fi Hotspots and Mobile Routers. On the external side, the RD can be connected to any type of medium (e.g. Cellular, Wi-Fi, SATCOM, Ethernet) to gain access to a Wide Area Network. On the internal side the RD is connected to EUDs either through an Ethernet cable or Wi-Fi. When the RD is a Wi-Fi access point connected to the EUD (or multiple EUDs), the Wi-Fi network shall implement Wi-Fi Protected Access II (WPA2) with either Pre-Shared Key (PSK) or WPA2 Enterprise. The EUD shall be configured to only permit connections to authorized RDs. RDs are only permitted to establish connectivity to the Black network, and may not be placed between an Outer Encryption Component and Inner Encryption Component.

The CP also allows connectivity without the use of a RD or physically separate VPN Gateway if any of the following Transport Networks are utilized: Domestic Cellular Providers, Government Private Cellular Networks, or Government Private Wireless Networks. Domestic Cellular Providers enable connectivity through cellular Base Stations geographically located within the United States of America. Government Private Cellular Networks are defined as cellular Base Stations which are owned and operated exclusively by the United States Government (such as in Tactical Environments). Finally, Government Private Wireless Networks denotes Wi-Fi connectivity by a Wireless Local Area Network (WLAN) accredited by a Government Authorizing Official (AO). These Wi-Fi networks must comply with applicable organization policies. Within the Department of Defense (DOD) the applicable policy is DOD Instruction (DODI) 8420.01. At a minimum these Wi-Fi networks must implement WPA2 with PSK; however, WPA2 with certificate-based authentication is preferred. When Government Private Wireless Networks utilize certificate-based authentication, they cannot share the Outer Tunnel CA or Inner Tunnel CA certificate management services. WPA2 protects the Black transport network, but does not count as one of the layers of CSfC Data-in-Transit encryption.

Finally, the CP allows connectivity without a RD or physically separate VPN Gateway when implementing the VPN EUD Solution Design connecting through a Wired Internet connection (e.g. Residential Internet connection using Ethernet between the EUD and a Router).

Table 2. Acceptable Black Transport Networks

	VPN EUD	TLS EUD
Any Black Transport Network	Government RD **OR** VPN Gateway	Government RD **OR** VPN Gateway
Domestic Cellular, Government Private Cellular, or Government Private Wireless	No additional requirements	No additional Requirements
Wired Internet Connection	No additional requirements	No additional Requirements

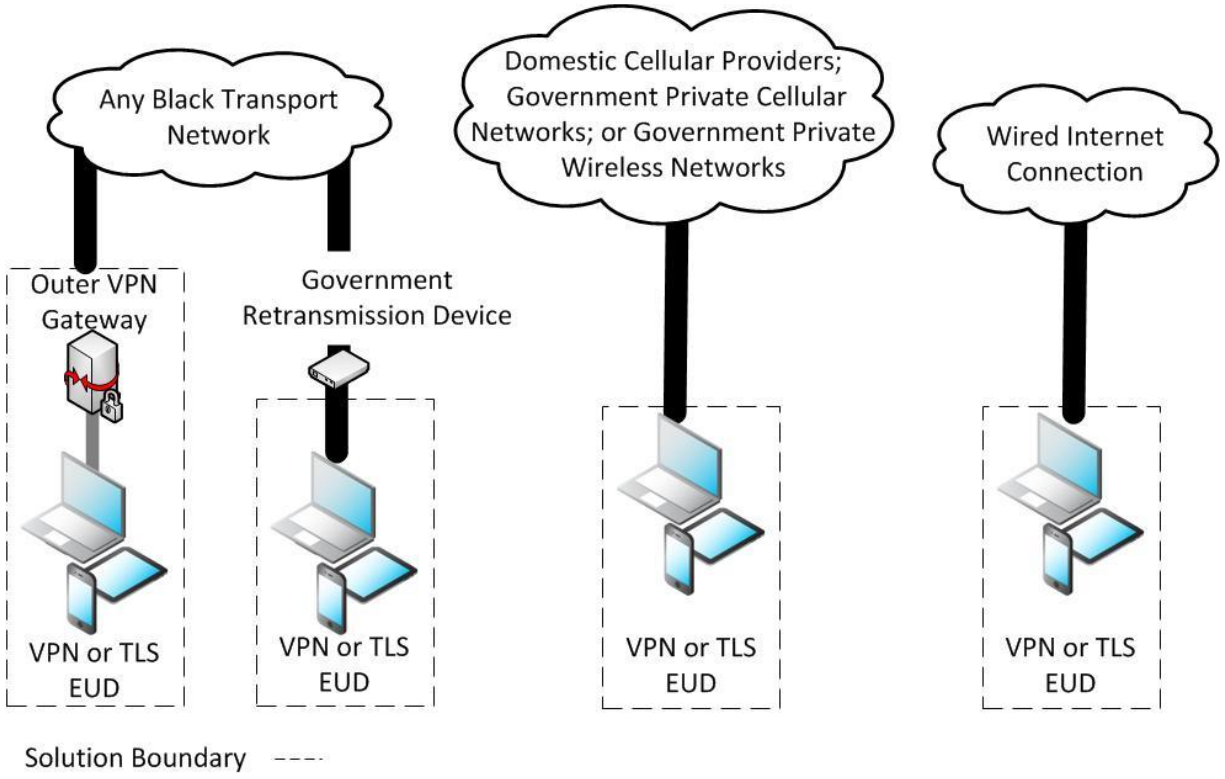

Figure 2. Acceptable Black Transport Networks

As shown in Figure 2, both EUD designs can connect to the Mobile Access solution over Domestic Cellular, Government Private Cellular, or Government Private Wireless Networks without the need for a separate standalone piece of hardware. Additionally, when a VPN EUD uses a Wired Internet connection there is no need for a separate, standalone piece of hardware. When connecting over any other black transport network, EUDs must use a standalone VPN Gateway or a Government RD to connect to the Mobile Access Solution. When an EUD includes a standalone VPN Gateway, that

Gateway is utilized to establish the Outer Layer of IPsec to the government infrastructure and is included within the CSfC Solution Boundary. Additionally, the VPN Gateway must be wired to the computing platform which terminates the Inner layer of encryption. Although only required as described above, a standalone VPN Gateway can be utilized for any of the EUD Solution designs to connect to any transport network. Similarly, an EUD can utilize a Government RD to connect to any transport network. The Government RD is outside the CSfC Solution Boundary, but acts as an intermediary between the desired transport network and the EUD.

4.1.4 DATA, MANAGEMENT, AND CONTROL PLANE TRAFFIC

Data plane traffic is classified information, encrypted or not, that is being passed through the MA solution. The MA solution exists to encrypt and decrypt data plane traffic. All data plane traffic within the Black network is encapsulated within the Encapsulating Security Payload (ESP) protocol. All data plane traffic within the Gray network is encapsulated within ESP, TLS, or SRTP.

Management plane traffic is used to configure and monitor solution components. It includes the communications between a system administrator and a component, as well as the logs and other status information forwarded from a solution component to a SIEM or similar repository. Management plane traffic on Red and Gray networks is encapsulated within the Secure Shell version 2 (SSHv2), ESP, or TLS protocol.

Control plane traffic consists of standard protocols necessary for the network to function. Control plane traffic is typically not initiated directly on behalf of a user (unlike data traffic) or a system administrator (unlike management traffic). Many, but not all, control plane protocols operate at Layer 2 or Layer 3 of the Open Systems Interconnection (OSI) model. Examples of control plane traffic include, but are not limited to, the following:

- Network address configuration (e.g. Dynamic Host Configuration Protocol (DHCP), Neighbor Discovery Protocol (NDP), etc.)
- Address resolution (e.g. Address Resolution Protocol (ARP), NDP, etc.)
- Name resolution (e.g. Domain Name System (DNS), etc.)
- Time synchronization (e.g. Network Time Protocol (NTP), Precision Time Protocol (PTP), etc.)
- Route advertisement (e.g. Routing Information Protocol (RIP), Open Shortest Path First (OSPF), Intermediate System to Intermediate System (IS-IS), Border Gateway Protocol (BGP), etc.)
- Certificate status distribution (e.g. Online Certificate Status Protocol (OCSP), HTTP download of CRLs, etc.)

The MA CP explicitly prohibits the use of most control plane traffic for EUDs consisting of a single computing device to provide both the Inner and Outer layer of encryption (see Appendix D). The MA CP does not allow route advertisement or certificate status distribution to ingress/egress from the Black Transport Network for these EUDs. As a result, the implementing organization will require procedures to be in place to handle a situation in which the certificate of an Outer VPN Gateway is revoked. EUDs are configured to enable all IP traffic, with the exception of network Internet Key Exchange (IKE), address configuration, time synchronization, and name resolution traffic, to flow through the Outer IPsec VPN Client. EUDs selected from the CSfC Components List can ensure that IP traffic flows through the Outer IPsec VPN Client by placing the device in the NIAP evaluated configuration. Upon establishing the Outer VPN tunnel, the CP does not impose detailed requirements restricting control plane traffic in the Gray and Red networks.

Restrictions are also placed on control plane traffic for the Outer VPN Gateway. The Outer VPN Gateway is prohibited from implementing routing protocols on external and internal interfaces. The Outer VPN Gateway can rely on the Outer firewall to perform routing functionality.

Except as otherwise specified in this CP, the usage of specific control plane protocols is left to the solution owner to approve, but any control plane protocols not approved by the solution owner must be disabled or blocked.

Data plane and management plane traffic are generally required to be separated from one another by using physical or cryptographic separation. Use of a Virtual Local Area Network (VLAN) alone is not sufficient to separate data plane and management plane traffic. As a result, a solution may, for example, have a Gray Data network and a Gray Management network which are separate from one another, where the components on the Gray Management network are used to manage the components on the Gray Data network. The Gray Management network is separated from the Gray Data network via the Gray firewall. The Gray firewall utilizes an ACL to ensure that only appropriate Gray Management Services (i.e. Administration Workstation, SIEM or Network Time Server) can communicate with the Outer VPN Gateway and EUDs that have established an Outer VPN tunnel. Given that some control plane traffic is necessary for a network to function, there is no general requirement that control plane traffic be similarly separated, unless otherwise specified.

4.2 High-Level Design

The MA solution is adaptable to support multiple capabilities, depending on the needs of the customer implementing the solution. The supported EUD capabilities are mutually exclusive, therefore if a customer chooses to implement an EUD using two layers of IPsec, then the Inner TLS Client would not be included as part of that EUD implementation. Similarly, if a customer only needs a Secure Voice Capability, then the Inner IPsec Component would not be included as part of that EUD implementation. Although the EUD Solution Designs are mutually exclusive, the infrastructure may be configured to support both EUD solution designs (see Appendix D). This enables implementation of both types of

EUDs based on use cases and device features. Any implementation of the MA solution must satisfy all of the applicable requirements specified in this CP, as explained in sections 12 and 13.

4.2.1 End User Devices

This CP uses the concept of an EUD, which includes a computing device such as a smart phone, laptop, or tablet. The EUDs provide two layers of protection for data in transit to tunnel through the black network and access classified data on the Enterprise/Red network. In some instances, an EUD encompasses more than one piece of hardware (e.g. Computing Device and VPN Gateway) each of which perform a layer of encryption. Where more than one piece of hardware is used, each component is included as part of the EUD and are within the CSfC Solution Boundary. There are two EUD designs which can be implemented as part of a MA solution. Each of the EUD designs share many requirements in common, but also have unique requirements specific to that design:

1) **IPsec-IPsec (VPN EUD):** Utilizes two IPsec tunnels to connect to the Enterprise/Red network. Such an EUD includes both an Inner VPN Client and Outer VPN Component to provide the two layers of IPsec. Throughout the document this EUD design is referred to as the "VPN EUD". VPN EUDs can be implemented utilizing combinations of IPsec VPN Clients and IPsec Gateways (see Appendix D). For example, a VPN EUD can be implemented on a computing device with two VPN Clients running on separate IP stacks. Similarly, the MA CP allows a VPN EUD to utilize a VPN Gateway to provide the Outer layer of IPsec encryption and a VPN Client installed on a computing device to provide the Inner layer of encryption.

2) **IPsec-TLS (TLS EUD):** Utilizes an Outer layer of IPsec encryption and an Inner layer of TLS encryption to access the Enterprise/Red network. Throughout the document this EUD design is referred to as "TLS EUD". The Outer layer of encryption can be provided by either an IPsec VPN Client or a standalone IPsec VPN Gateway. The Inner layer of encryption is then provided by a TLS Client. The EUD TLS Client includes a number of different options which can be selected, in accordance with the CP requirements, to meet the operational needs of the customer. The EUD TLS Clients include, but are not limited to, Web Browsers, Email Clients, and VoIP Applications. Traffic between the TLS EUD Client and the TLS-Protected Server is encrypted with TLS or in some instances SRTP. When SRTP is utilized, session keys are first exchanged using Session Initiation Protocol (SIP) over TLS.

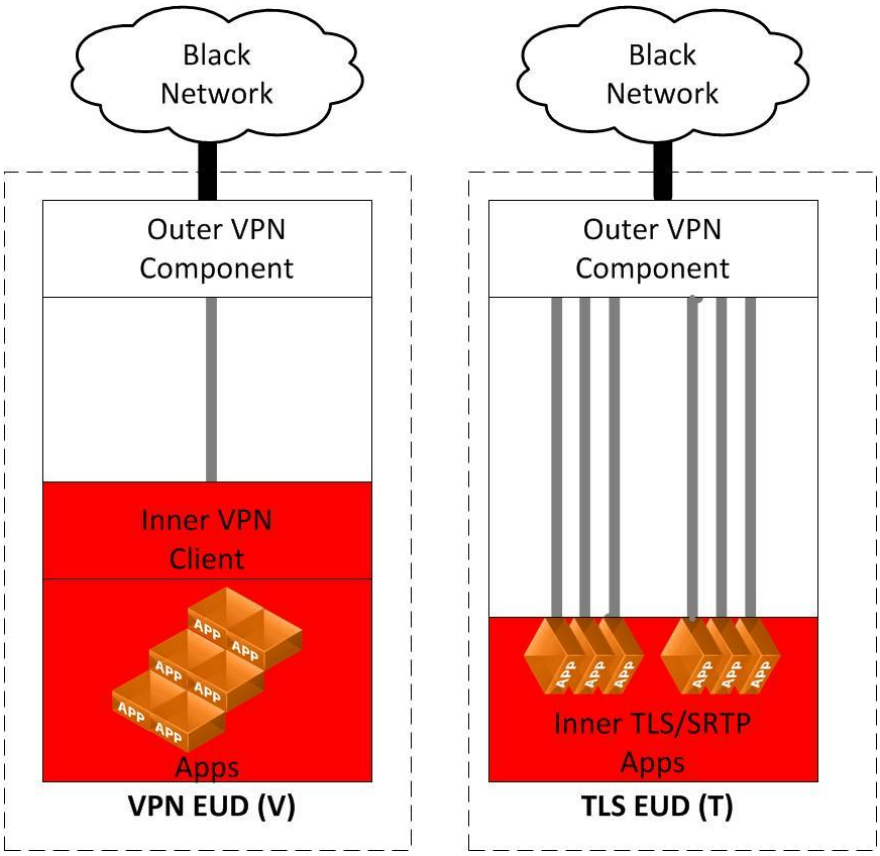

Figure 3. EUD Solution Designs

Figure 3 depicts the two EUD Solution Designs available as part of the MA CP. In each design the Outer VPN Component is utilized to establish an IPsec tunnel to the Outer VPN Gateway of the Mobile Access Solution infrastructure. In either EUD design this Outer VPN Component could be either a VPN Client or a VPN Gateway selected from the CSfC Components List. If a standalone VPN Gateway is utilized to provide the Outer IPsec tunnel, then it must be wired directly to the EUD (i.e. Ethernet cable).

The Inner layer of encryption for VPN EUDs is provided by a VPN Client. The Inner VPN Client must be selected from the CSfC Components List (see Section 12). If VPN Clients are used for both the Inner and Outer layers of encryption then they must utilize a different IP stack, and generally are implemented using Virtualization.

The Inner layer of encryption for TLS EUDs is provided by either TLS or SRTP. Every application which performs TLS or SRTP must be selected from the CSfC Components List.

The Mobile Access CP allows three different deployment options pertaining to the use and handling of an EUD while powered off:

1. **EUD with DAR:** To implement Data-at-Rest on an EUD, the DAR solution shall be approved by NSA – either as a tailored solution, or compliant with NSA's Data at Rest Capability Package (DAR CP) for the protection of information classified at the level of the Enterprise/Red network connected to the EUD. Specification of such a DAR solution is outside the scope of this CP, but can be found in the Data at Rest CP. Positive control of the EUD must be maintained at all times. The EUD is considered lost if out of positive control for twenty (20) minutes or more where positive control is defined by the AO.

2. **Thin EUD:** The EUD can be designed to prevent any classified information from being saved to any persistent storage media on the EUD. Possible techniques for implementing this include, but are not limited to: using VDI configured not to allow data from the Enterprise/Red network to be saved on the EUD, restricting the user to a non-persistent virtual machine on the EUD, and/or configuring the EUD's operating system to prevent the user from saving data locally. Since the EUD does not provide secure local storage for classified data, its user is also prohibited by policy from saving classified data to it. The EUD in this case must enable the native platform DAR protection to protect the private keys stored on it from disclosure and to increase the difficulty of tampering with the software and configuration. This option is not permitted if any of the private keys or certificates stored on the EUD are considered classified by the AO. Positive control of the EUD must be maintained at all times. The EUD is considered lost if out of positive control for twenty (20) minutes or more where positive control is defined by the AO.

3. **Classified EUD:** The EUD can be used exclusively with physical security measures approved by the AO. EUDs are not subject to special physical handling restrictions beyond those applicable for classified devices, since they can rely on the environment they are in for physical protection. If this design option is selected, then the EUDs must be treated as classified devices at all times. The EUD in this case must enable the native platform DAR protection to protect the private keys stored on it from disclosure and to increase the difficulty of tampering with the software and configuration. Positive control of the EUD must be maintained at all times. The EUD is considered lost if out of positive control for twenty (20) minutes or more where positive control is defined by the AO.

While powered on, an EUD is classified at the same level of the Enterprise/Red network that it communicates with through the MA solution, since classified data may be present in volatile memory and/or displayed on screen. To mitigate the risk of accidental disclosure of classified information to unauthorized personnel while the EUD is in use, the customer must define and implement an EUD user agreement that specifies the rules of use for the system. The customer must only grant users access to

an EUD after they agree to the user agreement and receive training on how to use and protect their EUD. There is no limit to the number of EUDs that may be included in a MA solution.

4.2.2 INDEPENDENT SITE

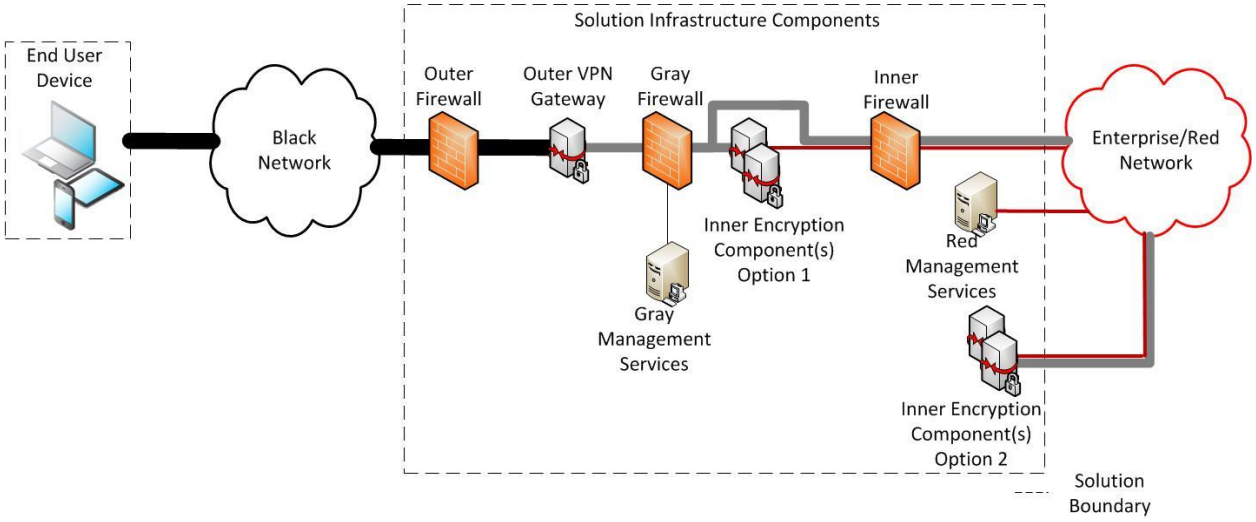

Figure 4. EUDs Connected to Independent Site

Figure 4 depicts a single Red network connected to EUDs that operate at the same security level, through the MA solution. Here, the Enterprise/Red network has at least two Encryption Components associated with it: One or more Inner Encryption Components connected to the Red network, and an Outer VPN Gateway between the Inner Encryption Components and the Black network. The Inner Encryption Component(s) can terminate either in the Grey network as depicted in Option 1 or within the Enterprise/Red network as depicted in Option 2. There are two layers of encryption between any EUD communicating with the Enterprise/Red network: one IPsec tunnel between their Outer VPN Components, and a second IPsec, TLS or SRTP tunnel depending on the selected EUD Design(s).

For independent sites, administration is performed at that site for all components within the Solution Boundary including the Outer VPN Gateway, Gray Management Services, Inner Encryption Components, Red Management Services, firewalls, and EUDs. Independent Sites are not interconnected with other Infrastructure Sites through the MA Solution. Therefore management, data plane, and control plane traffic between Solution Infrastructure sites are outside the scope of the MA CP. If two or more sites must be interconnected, customers may also register the MA solution against the VPN CP or utilize an NSA-Certified encryptor.

Note that while Figure 4 depicts only a single EUD, this solution does not preclude the use of a large number of EUDs being implemented.

4.2.3 MULTIPLE SITES

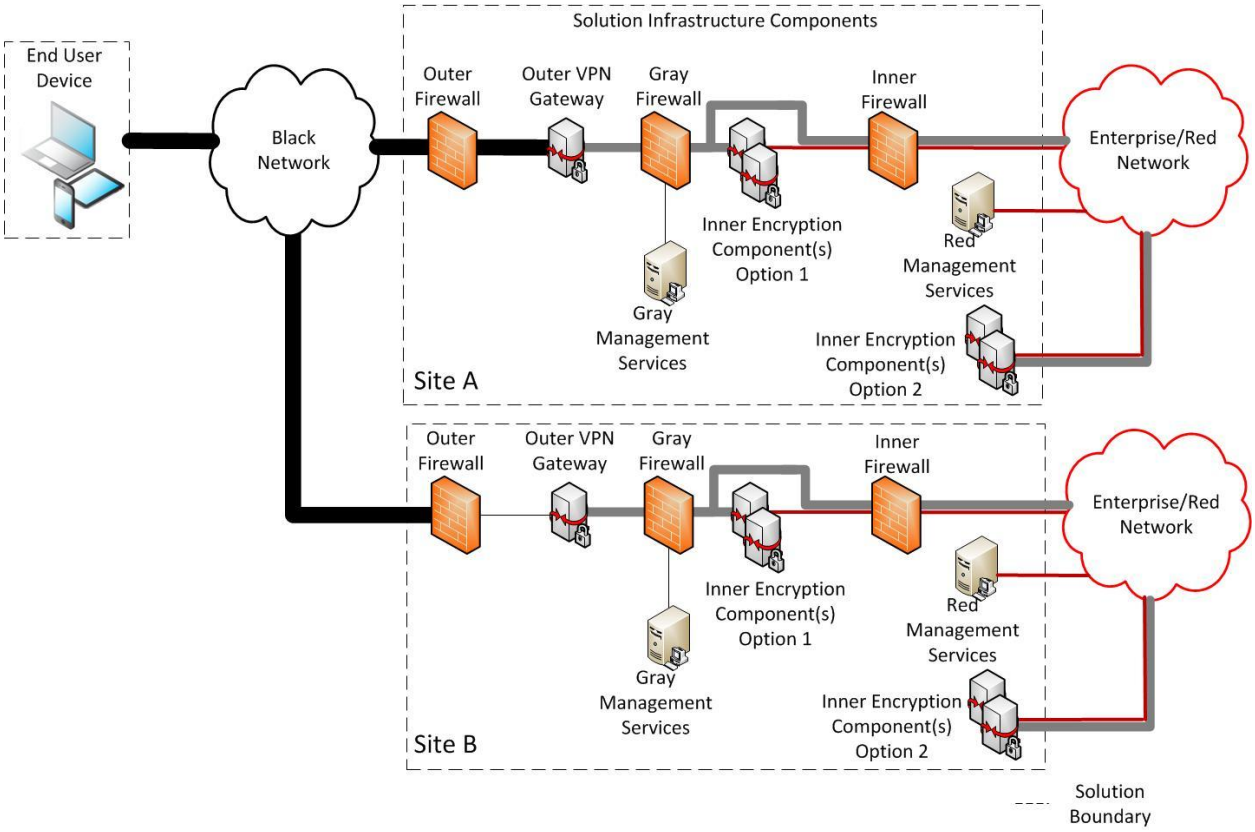

Figure 5. Multiple Mobile Access Solution Infrastructures supporting EUDs

Figure 5 depicts two MA Solution Infrastructures which an EUD can connect to in order to access Enterprise/Red network services. Customers may want to implement multiple Solution Infrastructures to support Continuity of Operations or provide better performance based on geographic location of EUDs or Enterprise/Red services. The Multiple Solution Infrastructures may be interconnected using a NSA-approved solution such as the Virtual Private Network (VPN) CP or a NSA-Certified encryptor; however, connectivity of Solution Infrastructure Components is outside the scope of the MA CP.

Note that, while Figure 5 depicts only two sites, this solution can scale to include numerous sites, with each additional site having the same design as those in the figure.

4.3 RATIONALE FOR LAYERED ENCRYPTION

A single layer of Suite B encryption, properly implemented, is sufficient to protect classified data in transit across an untrusted network. The MA solution uses two layers of Suite B encryption not because

of a deficiency in the cryptographic algorithms themselves, but rather to mitigate the risk that a failure in one of the Components, whether by accidental misconfiguration, operator error, or malicious exploitation of an implementation vulnerability results in exposure of classified information. The use of multiple layers of protection reduces the likelihood of any one vulnerability can be used to exploit the full solution, particularly if the layers exhibit suitable independence.

If an Outer VPN Component is compromised or fails in some way, the Inner Encryption Component can still provide sufficient encryption to prevent the immediate exposure of classified data to a Black network. In addition, the Gray firewall can indicate that a failure of the Outer VPN Gateway has occurred, since the filtering rules applied to its external network interface will drop and log the receipt of any packets not associated with an Inner Encryption Component. Such log messages indicate that the Outer VPN Gateway has been breached or misconfigured to permit traffic to pass through to the Inner Encryption Component that is not allowed.

Conversely, if instead the Inner Encryption Component is compromised or fails in some way, the Outer VPN Gateway can likewise provide sufficient encryption to prevent the immediate exposure of classified data to a Black network. As in the previous case, the Gray firewall filtering rules applied to its internal network interfaces will drop and log the receipt of any packets not associated with an Inner Encryption Component. Such log messages indicate that the Inner Gateway has been breached or misconfigured to permit traffic to pass through to the Outer VPN Gateway that is not allowed.

If both the Outer and Inner Gateways are both compromised or fail simultaneously, then it may be possible for classified data from the Enterprise/Red network to be sent to a Black network without an adequate level of encryption. The security of the MA solution depends on preventing this failure mode by promptly remediating any compromises or failures in one Encryption Component before the other also fails or is compromised.

Diversity of implementation is needed between the components in each layer of the solution in order to reduce the likelihood that both layers share a common vulnerability. The CSfC Program recognizes two ways to achieve this diversity. The first is to implement each layer using components produced by different manufacturers. The second is to use components from the same manufacturer, where that manufacturer has provided NSA with sufficient evidence that the implementations of the two components are independent of one another. The CSfC web page (http://www.nsa.gov/ia/programs/csfc_program) contains details for how a manufacturer can submit this evidence to NSA and what documentation must be provided. Customers wishing to implement a solution in accordance with this CP that uses products from the same manufacturer in both layers should contact their NSA/IAD Client Advocate to confirm that NSA has accepted the manufacturer's claims before implementing their solution.

4.4 AUTHENTICATION

The MA solution provides mutual device authentication between Outer VPN components and Inner Encryption components via public key certificates. This CP requires all authentication certificates issued to Outer VPN components and Inner Encryption components be Non-Person Entity (NPE) certificates, except in the case when TLS EUDs are implemented. Following the two layers of device authentication, VPN EUDs require the user to authenticate to the network before gaining access to any classified data. TLS EUDs typically utilize a user certificate to authenticate to TLS-Protected Server(s). In these instances, the user certificate authenticates the Inner layer of TLS encryption as well as authenticating the user for access to the requested classified data. Although not as common, TLS EUDs can be implemented using mutual device authentication between Outer and Inner Encryption components, similar to VPN EUDs. Following the two layers of device authentication, the user must then authenticate to the network before gaining access to any classified data.

In addition to authentication for the Outer and Inner layer of Encryption, the MA CP requires user-to-device authentication. This authentication occurs between the user and the Computing Device (which processes Red data) of an EUD. In some instances the computing device may be physically separate from the component of the EUD which provides the Outer layer of encryption (for example, a VPN Gateway provides the Outer Layer of encryption). The MA CP requires EUD components to utilize a minimum of a four-character, case–sensitive, alpha-numeric password to authenticate to the device. This password can be used both for decrypting the Platform Encryption as well as for unlocking the screen. EUD components, which are selected from the Mobile Platform section of the CSfC Components, are able to utilize a relatively short authentication factor since they are backed by a hardware root of trust which is evaluated during the NIAP certification.

The MA CP defines requirements for an Outer CA to issue NPE (i.e. device) authentication certificates to Outer VPN Components. The CP also defines requirements for an Inner CA to issue NPE authentication certificates to VPN EUDs and Inner VPN Gateways. TLS EUDs and TLS-Protected Servers primarily utilize User Authentication Certificates issued by an Inner CA. These User certificates are generally issued by the CA that is responsible for issuing enterprise server certificates, which may be different than the Inner CA described within this MA CP.

4.5 OTHER PROTOCOLS

Throughout this document, when IP traffic is discussed, it can refer to either IPv4 or IPv6 traffic, unless otherwise specified. In addition, Red, Gray and Black networks can run either IPv4 or IPv6 and each network is independent from the others in making that decision. In the remainder of the document, if no protocols or standards are specified then any appropriate protocols may be used to achieve the objective.

Public standards conformant Layer 2 control protocols such as ARP are allowed as necessary to ensure the operational usability of the network. This CP is agnostic with respect to Layer 2; specifically, it does not require Ethernet. Public standards conformant Layer 3 control protocols such as Internet Control Message Protocol (ICMP) may be allowed based on local AO policy, but the default configuration of this solution is for all Layer 3 control protocols to be disabled. Red and Gray network multicast messages and Internet Group Management Protocol (IGMP) or Multicast Listener Discovery (MLD) may also be allowed depending on local AO policy. Multicast messages received on external interfaces of the Outer VPN component shall be dropped.

It is expected that the MA solution can be implemented in such a way as to take advantage of standards-based routing protocols that are already being used in the network. For example, networks that currently use Generic Routing Encapsulation (GRE) or OSPF protocols can continue to use these in conjunction with this solution to provide routing as long as the AO approves their use.

4.6 AVAILABILITY

The high-level designs described in Section 4.2 are not designed with the intent of automatically providing high availability. Supporting solution implementations for which high availability is important is not a goal of this version of the CP. However, this CP does not prohibit adding redundant components in parallel to allow for component failover or to increase the throughput of the MA solution, as long as each redundant component adheres to the requirements of this CP. The CP does not limit the number of Outer VPN Gateways or Inner Encryption components which can be implemented for high availability in a MA Solution.

5 INFRASTRUCTURE COMPONENTS

In the high-level designs discussed in the previous section, all communications flowing across a Black network are protected by at least two layers of encryption, implemented using an outer IPsec VPN tunnel and an Inner layer of IPsec, TLS, or SRTP encryption. Mandatory aspects of the solution infrastructure also include Administration Workstations, IDS or IPS, Security Information Event Management (SIEM), firewalls, and CAs for key management using Public Key Infrastructure (PKI).

Each infrastructure component is described in more detail below. The descriptions include information about the security provided by the components as evidence for why they are deemed necessary for the solution. Components are selected from the CSfC Component List in accordance with the Product Selection requirements of this CP (see Section 12).

This section also provides details on additional components that can be added to the solution to help reduce the overall risk. However, where indicated in the text, these are not considered mandatory components for the security of the solution; therefore, this CP does not place configuration requirements on those optional components.

5.1 OUTER FIREWALL

Configuration and enforcement of network packet handling rules is fundamental to the security provided by the MA Solution Firewalls. The Outer firewall is located at the edge of the Mobile Access Solution Infrastructure and is connected to the Black Transport Network. The External Interface of the Outer firewall only permits IPsec IKE and ESP traffic with a destination address of the Outer VPN Gateway and AO-approved control plane traffic. The Internal Interface of the Outer firewall only permits IPsec traffic with a source address of the Outer VPN Gateway, AO-approved control plane traffic, and AO-approved Management Traffic. The minimum filtering required by the Outer firewall is primarily based on source IP addresses, source ports, destination IP addresses, and destination ports (see Section 13.9).

Although the Outer firewall is located on the perimeter of the network and thus more exposed to external attacks, the Outer firewall rules prohibit unauthorized data flows, which helps mitigate Denial of Service (DoS) attacks and resource exhaustion. This solution does not require that a single Outer firewall be utilized; however, all firewalls implemented as part of the Mobile Access Solution shall conform to the port filtering requirements in Section 13.9.

In addition to performing the functions described in this CP, the Outer firewall may also use AO-approved routing protocols on the Black network with the exception of prohibited control plane traffic as described in this CP. The Outer Firewall, selected from the CSFC Components List, must be physically separate from the Outer VPN Gateway as depicted in Figure 4.

5.2 OUTER VPN GATEWAY

Authentication of peer VPN Components, cryptographic protection of data in transit, and configuration and enforcement of network packet handling rules are all aspects fundamental to the security provided by VPN Gateways.

The external interface of the Outer VPN Gateway is connected to the internal interface of the Outer firewall. The VPN Gateway establishes an IPsec tunnel with peer Outer VPN Components, which provides device authentication, confidentiality, and integrity of information traversing Black networks. VPNs offer a decreased risk of exposure of information in transit since any information that traverses a Black network is placed in a secure tunnel that provides an authenticated and encrypted path between the site and an EUD. The Outer VPN Gateway is implemented identically for all the high-level designs, including when implemented as the Outer VPN Component for EUDs (see Section 6.1.1). Similar to the Outer firewall, the external interface of the Outer VPN Gateway only permits IPsec traffic and AO-approved control plane traffic. The internal interface of the Outer VPN Gateway is configured to only permit traffic with an IP address and port associated with Inner Encryption Components, Gray Management Services (i.e. SIEM and Administration Workstation), or Control Plane Component (i.e. DNS and NTP Servers in the Gray).

The Outer VPN Gateway is prohibited from implementing routing protocols on external and internal interfaces. The Outer VPN Gateway can rely on the Outer firewall and/or Gray firewall to perform routing functionality. The Outer VPN Gateway, selected from the CSFC Components List, must be physically separate from the Outer firewall and Gray firewall as depicted in Figure 4.

The Outer VPN Gateway cannot route packets between Gray and Black networks; any packets received on a Gray network interface and sent out a Black network interface must be transmitted within an IPsec VPN tunnel configured according to this CP.

For load balance or other performance reasons, multiple Outer VPN Gateways that comply with the requirements of the CP are acceptable.

5.3 GRAY FIREWALL

Gray firewalls are responsible for filtering traffic to only allow the proper traffic to flow to/from the Inner Encryption Components, Outer VPN Gateway, and Gray Management Services. Since this filtering is primarily based on the source and destination ports and addresses in the packet, the Gray networks themselves must use an addressing scheme that supports the necessary filtering (such as using separate address ranges for the Gray interfaces of Inner Encryption Components supporting different TLS-Protected Server devices). The Gray firewalls are configured to only allow the necessary type of traffic based on the type(s) of EUD Design implemented. For example, the Gray firewall will only allow valid IP addresses or address ranges to perform DNS queries to a Gray DNS server.

For load balance or other performance reasons, multiple Gray firewalls that comply with the requirements of the CP are acceptable. The Gray firewall, selected from the CSFC Components List, must be physically separate from the Outer VPN Gateway and Inner Encryption Components as depicted in Figure 4.

5.4 GRAY MANAGEMENT SERVICES

Secure administration of components in the Gray network and continuous monitoring of the Gray network are essential roles provided by the Gray Management Services. Gray Management Services are composed of a number of components which each can play a distinct role in the overall security of the solution. The MA CP allows flexibility in the placement of some Gray Management Services as described below. All components within the Gray Management Services are either connected directly to the Gray firewall or indirectly connected to the Gray firewall (i.e. multiple Gray Management Services connected to a switch which is connected to the Gray firewall). Finally, the Gray Management Services are physically protected as classified devices.

5.4.1 OUTER CERTIFICATE AUTHORITY (LOCATED ON GRAY NETWORK)

An Outer CA located on the Gray network issues digital certificates for the Outer VPN Components in the solution. These certificates are used for authentication in establishing the Outer IPsec tunnels between

pairs of VPN Components. If an Outer CA is located in the Gray network then the CP also requires a physically separate Inner CA located in the Enterprise/Red network. The Inner CA issues certificates to the Inner Encryption Components. This separation provides key management separation between the two independent layers of encryption.

To improve integration with existing Enterprise PKI and enable remote renewal of EUD Certificates, the MA CP allows for flexibility in the placement of Certificate Authorities. As an alternative to implementing the Outer CA as a Gray Management Service, customers can choose to implement the Outer CA on the Enterprise/Red network (See Section 9). When the Outer CA is located in the Enterprise/Red network it is not managed by the Gray Management Services.

5.4.2 Gray Administration Workstation

The Gray Administration Workstations is responsible for maintaining, monitoring, and controlling all security functionality for the Outer VPN Gateway, Gray firewall, and all Gray Management Service components. The Gray Administrative Workstations are not permitted to maintain, monitor, or control Inner Encryption Components or Red Management Services. All Mobile Access Solutions will have at least one Gray Administrative Workstation. Section 7 provides more detail on management of Mobile Access Solution components.

5.4.3 Gray Certificate Revocation Services

CRL Distribution Points (CDP) and Online Certificate Status Protocol (OCSP) Responders are servers other than a CA that makes revocation information available to components. Outer CDPs and OCSP Responders are deployed on the internal side of the Outer VPN Gateway for which revocation information is being made available. Collectively Outer CDPs and OCSP Responders are referred to as Gray Certificate Revocation Services. The Gray Certificate Revocation Services ensure the Outer VPN Gateway can verify the status of the certificates used by the Outer VPN Component of EUDs. The Gray Certificate Revocation Services also provide certificate revocation information to Gray Management Services.

CDPs and OCSP Responders are not required components of the Mobile Access CP, but if not utilized the organization must implement other means, such as whitelists, to ensure that once a certificate is revoked it cannot successfully establish an Outer IPsec Tunnel with the Solution Infrastructure. The Mobile Access CP also allows for an Inner CDP to be stood up in the Gray Management Services. Placing an Inner CDP in the Gray Management services allows EUDs to check the certificate status of the Inner Encryption component prior to establishing a tunnel. To utilize an Inner CDP in the Gray Management Services, an AO must determine that CRLs generated by the Inner CA are unclassified. Additionally, these CRLs must be moved from the Enterprise/Red network to the Gray Management Services using an AO approved method (e.g. Cross Domain Solution).

The use of CDPs in a Mobile Access Solution is discussed in detail in Section 9.1.

5.4.4 Gray Security Information and Event Management (SIEM)

The Gray SIEM collects and analyzes log data from the Outer VPN Gateway, Gray firewall, and other Gray Management Service components. Log data may be encrypted between the originating component and the Gray SIEM with SSHv2, TLS, or IPsec to maintain confidentiality and integrity of the log data. At a minimum, an auditor reviews the Gray SIEM on a weekly basis. The SIEM is configured to provide alerts for specific events including if the Outer VPN Gateway or Gray firewall receive and drop any unexpected traffic which could indicate a compromise of the Outer firewall or Outer VPN Gateway respectively. These functions can also be performed on an Enterprise/Red SIEM if AO-approved one-way taps are utilized as described in this CP (see Section 8.2).

5.5 Inner Encryption Components

The MA CP allows for the use of up to three different types of Inner Encryption Components: Inner VPN Gateway, Inner TLS-Protected Server, or Inner SRTP Endpoint. Inner VPN Gateways are always located between the Gray firewall and Inner firewall. An Inner VPN Gateway will always have at least two interfaces. One external interface connected to the Gray firewall and one internal interface connected to the Inner firewall.

Inner TLS-Protected Servers and Inner SRTP Endpoints are permitted to use a single interface or multiple interfaces. Similar to the Inner VPN Gateway, Inner TLS-Protected Servers and SRTP Endpoints with multiple interfaces can have one external interface connect to the Gray firewall and one internal interface connected to the Inner firewall. If implemented with a single interface, then that interface establishes the Inner layer of encryption and provides the classified data to the TLS EUD. An example of a TLS-Protected Server with a single interface is a web server on the Enterprise/Red network which terminates the Inner layer of encryption with HTTPS and directly returns the content to the TLS EUD. An example of a SRTP Endpoint with a single interface is a VoIP Desktop Phone in the Enterprise Network which terminates the SRTP encryption and sends the voice traffic from the VoIP Desktop Phone. The TLS-Protected Servers and SRTP Endpoints can be placed either between the Gray firewall and Inner firewall or within the Enterprise/Red network.

A MA Solution Infrastructure may support both TLS EUDs and VPN EUDs. When supporting both TLS EUDs and VPN EUDs the solution infrastructure will always include an Inner VPN Gateway between the Gray firewall and Inner firewall. This Inner VPN Gateway will terminate the Inner layer of IPsec traffic for all VPN EUDs. Additionally, the solution infrastructure will include one or more TLS-Protected Servers. The TLS-Protected Servers are either placed between the Gray firewall and Inner firewall or on the internal side of the Inner firewall. When placed between the Gray firewall and Inner firewall the TLS-Protected Server(s) must be placed in parallel with the Inner VPN Gateway such that the TLS-Protected Server is not dependent on the Inner-VPN Gateway to reach the Gray firewall or Inner firewall. When the solution includes a TLS-Protected Server located in the Enterprise/Red network the Gray firewall includes a physical path directly to the Inner firewall. Proper configuration of the Gray

firewall and Inner firewall ACL is critically important when supporting TLS-Protected Servers in the Enterprise. The Gray firewall must ensure that only packets destined for the IP address of a TLS-Protected Server within the Solution Boundary are permitted to flow to the Inner firewall. Similarly, the Inner firewall must ensure that only packets destined for the IP address of a TLS-Protected Server within the Solution Boundary are permitted to the Enterprise/Red network (see Appendix D).

For load balance or other performance reasons, multiple Inner Encryption Components that comply with the requirements of the CP are acceptable.

5.5.1 INNER VPN GATEWAY

Similar to the Outer VPN Gateway, the Inner VPN Gateway provides authentication of peer VPN Components, cryptographic protection of data in transit, and configuration and enforcement of network packet handling rules. The Inner VPN Gateway is located between the Gray firewall and the Inner firewall. The Inner VPN Gateway is required to be implemented if supporting VPN EUDs.

The External Interface of the Inner VPN Gateway is connected to the internal interface of the Gray firewall. The VPN Gateway establishes an IPsec tunnel with peer Inner VPN Components, which provides a second layer of device authentication, confidentiality, and integrity of information traversing Black networks. Similar to the Outer VPN Gateway, the external interface of the Inner VPN Gateway only permits the egress of IPsec traffic and AO-approved control plane traffic. The internal interface of the Inner VPN Gateway is configured to only permit traffic with an IP address and port associated with Red network services.

The Inner VPN Gateway cannot route packets between Red and Gray networks; any packets received on a Red network interface and sent to a Gray network interface must be transmitted within an IPsec VPN tunnel configured according to this CP. The Inner VPN Gateway, selected from the CSFC Components List, must be physically separate from the Gray firewall and Inner firewall as depicted in Figure 4.

5.5.2 INNER TLS-PROTECTED SERVER

Inner TLS-Protected Server(s) utilizes TLS to provide confidentiality, integrity, and mutual authentication between an EUD and TLS-Protected Server. The TLS-Protected Server is either located between the Gray firewall and the Inner firewall or within an Enterprise/Red network. Inner TLS-Protected Servers are required to be implemented if supporting TLS EUDs.

This CP allows the TLS-Protected Server to utilize any protocol that is encapsulated in TLS. TLS-Protected Servers are selected from the CSfC Components List. All TLS-Protected Servers which terminate the Inner layer of encryption originating from a TLS EUD reside within the CSfC Solution Boundary, and therefore must meet all applicable requirements of the MA CP. This is true both of TLS-Protected Servers which are implemented specifically for the CSfC Solution as well as Enterprise/Red TLS-Protected Servers which terminate the inner tunnel originating from EUDs.

Examples of TLS-Protected Servers include, but are not limited to, Web Servers, SIP Servers, and Mobile Device Management (MDM) Servers. Web Servers implemented as part of the MA CP terminate the Inner layer of encryption utilizing HTTPS. SIP Servers utilize SIP over TLS for registration of EUDs and SRTP Endpoints, session setup, and session termination. When SIP Servers are included Session Description Protocol Security Descriptions (SDES) is used over the SIP TLS session for key exchange between TLS EUDs or between a TLS EUD and a SRTP Endpoint. The Inner TLS Protected-Server, selected from the CSFC Components List, must be physically separate from the Gray firewall and Inner firewall as depicted in Figure 4.

5.5.3 INNER SRTP ENDPOINT

Inner SRTP Endpoints provides cryptographic protection of data in transit. Within the MA Solution Infrastructure, SRTP Endpoints are either located between the Gray firewall and the Inner firewall or within an Enterprise Network. The Inner Layer of SRTP Encryption can also be terminated between two EUDs (see Section 6.3). Registration, session setup (including authentication and Key Exchange), and session termination for the SRTP Endpoints is performed utilizing SIP over TLS. Inner SRTP Endpoints are required to be implemented if supporting TLS EUDs that utilize SRTP.

All SRTP Endpoints which terminate the Inner layer of encryption originating from a TLS EUD reside within the CSfC Solution Boundary, and therefore must meet all applicable requirements of the MA CP. This is true for both of the SRTP Endpoints, which are implemented specifically for the CSfC Solution as well as Enterprise/Red SRTP Endpoints which terminate the inner tunnel.

Examples of Infrastructure SRTP Endpoints include VoIP Desktop Phones and VoIP Gateway/Border Controller (also known as Session Border Controllers). VoIP Desktop Phones generally reside within existing Enterprise Networks on the internal side of the Inner firewall. These Desktop Phones can provide end-to-end encryption of voice and/or video to TLS EUDs. VoIP Gateway/Border Controller terminates SRTP Traffic from a TLS EUD, and relay the data to the Enterprise/Red network. When a VoIP Gateway/Border Controller terminates the Inner layer of SRTP, Desktop Phones are not included in the Solution Boundary. Inclusion of a VoIP Gateway/Border Controller allows integration with existing enterprise voice systems.

The Inner SRTP Endpoint, selected from the CSFC Components List, must be physically separate from the Gray firewall and Inner firewall as depicted in Figure 4.

5.5.4 INNER FIREWALL

The Inner firewall is responsible for filtering to only allow the proper traffic to flow to/from the Enterprise/Red network. Since this filtering is primarily based on source and destination ports and addresses, the Inner Encryption components should use an addressing scheme that supports the necessary filtering. When the IInner layer of encryption is terminated by a TLS-Protected Server or SRTP Endpoint in the Enterprise/Red network, the Inner firewall must implement an ACL. The Inner firewall ACL is critical to ensure that only TLS-Protected Servers and SRTP Endpoints, which are configured in

accordance with this CP can terminate the Inner layer of encryption. A similar requirement is not placed on the Inner firewall when the the Inner layer of encryption terminates on an Inner VPN Gateway or TLS-Protected Server located between the Gray Firewall and Inner Firewall.

For load balance or other performance reasons, multiple Inner firewalls that comply with the requirements of the CP are acceptable.

5.6 RED MANAGEMENT SERVICES

Secure Administration of Inner Encryption Components and continuous monitoring of the Red network are essential roles provided by the Red Management Services. Red Management Services are composed of a number of components which can each play a distinct role in the overall security of the solution. The Mobile Access CP allows flexibility in the placement of some Red Management Services as described below.

5.6.1 CERTIFICATE AUTHORITIES (LOCATED ON RED NETWORK)

Mobile Access CP Solutions will always have at least one CA located in the Red network. At a minimum an Inner CA is included in the Red network to issue digital certificates for the Inner Encryption Components in the solution. These certificates are used for authentication in establishing the inner tunnel of encryption between pairs of Inner Encryption Components. The MA CP also allows Outer CAs to be included in the Red network to issue digital certificates for the Outer VPN Components. These certificates are used for device authentication in establishing the outer tunnel of encryption between pairs of VPN Components. When an Outer Tunnel CA is placed in the Red network it is critical to have AO-approved mechanisms in place to transfer revocation information to the Gray network in order to ensure it is accessible to the Outer VPN Gateway and Gray Management Services. When an Enterprise PKI capability is utilized, it is managed with existing processes and capabilities. Enterprise CAs then provide certificate management services for the MA solution over the Enterprise/Red network.

5.6.2 RED ADMINISTRATION WORKSTATIONS

The Red Administration Workstation is responsible for maintaining, monitoring, and controlling all security functionality for the Inner Encryption Components, Inner firewall, and all Red Management Service components. The Red Administrative Workstations are not permitted to maintain, monitor, or control Outer Encryption Components or Gray Management Services. All MA Solutions will have at least one Red Administrative Workstation. Section 7 provides more detail on management of Mobile Access Solution components.

5.6.3 RED SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

Red SIEMs collect and analyze log data from the Inner Encryption Components, the Inner firewall, and other Red Management Service components. Log data may be encrypted between the originating component and the Red SIEM with SSHv2, TLS, or IPsec to ensure confidentiality and integrity. At a minimum an auditor reviews the Red SIEM on a weekly basis. The SIEM is configured to provide alerts

for specific events including if the Inner Encryption Components or Inner firewall receive and drop any unexpected traffic which could indicate a compromise of the Gray firewall, Inner Encryption Components, or Inner firewall. While Red SIEMs are not a mandatory component of the MA Solution, customers are encouraged to leverage existing Enterprise SIEM capabilities to monitor log data from Inner Encryption Components, the Inner firewall, and Red Management Services. Although a Red SIEM is not required, it is still required to analyze logs from all Inner Encryption components on at least a weekly basis. A Red SIEM may also be utilized to analyze log data from Gray network components when utilized in conjunction with one-way taps as described in this CP (see Section 8.2).

5.6.4 RED CERTIFICATE REVOCATION SERVICES

CRL Distribution Points (CDP) and Online Certificate Status Protocol (OCSP) Responders are servers other than a CA that make revocation information available to components. Red CDPs and OCSP Responders are deployed either between the Inner Encryption Component and Inner firewall or on the internal side of the Inner firewall. Red CDPs and OCSP Responders make revocation information available to Inner Encryption Components of the Solution Infrastructure. Collectively Red CDPs and OCSP Responders are referred to as Red Certificate Revocation Services. The Red Certificate Revocation Services ensure the Solution Infrastructure Inner Encryption Components can verify the status of the certificates used by the Inner Encryption Components of EUDs.

CDPs and OCSP Responders are not required components of the Mobile Access CP, but if not utilized the organization must implement other means, such as whitelists, to ensure that, once a certificate is revoked, it cannot successfully establish an Inner Tunnel with the Solution Infrastructure.

6 END USER DEVICE COMPONENTS

The MA CP supports the use of two EUDs: VPN EUDs and TLS EUDs. The MA Solution Infrastructure can support both types of EUDs; however, the EUD must be dedicated as either a VPN EUD or TLS EUD. VPN and TLS EUDs are composed of a computing device and optionally include a physically separate VPN Gateway to provide the Outer Layer of IPsec encryption. When VPN Gateways are included as part of the EUD, they must be physically connected (i.e. Ethernet cable) to the computing device (see Figure 2).

A RD to connect to the Black network is also a required component, except for the solution designs and use cases specified in section 4.1.3. and 6.1.1.

6.1 OUTER VPN COMPONENT

The allowable Outer VPN Components for both the VPN and TLS EUD are identical. Authentication of peer VPN Components and cryptographic protection of data in transit are fundamental aspects to the security provided by the EUD Outer VPN Component Gateways.

The Outer VPN Component establishes an IPsec tunnel with the Solution Infrastructure Outer VPN Gateway, which provides device authentication, confidentiality and integrity of information traversing

Black networks. VPNs offer a decreased risk of exposure of information in transit since any information that traverses a Black network is placed in a secure tunnel that provides an authenticated and encrypted path between the EUD and the Mobile Access Solution Infrastructure. The Mobile Access CP allows the use of VPN Gateways or VPN Clients to be utilized as the Outer VPN Component of EUDs.

The private keys and certificates utilized for the authentication of the Outer VPN Component are considered Controlled Unclassified Information (CUI) and must be protected with at least FIPS 140-2-validated encryption. Customers deploying Mobile Access Solutions in high-threat environments may also choose to implement controls to mitigate against tampering attacks.

6.1.1 Outer VPN Gateway

An Outer VPN Gateway can be utilized as the Outer VPN Component for EUDs. Utilizing a physically separate VPN Gateway as part of the EUD improves security by providing physical separation between the computing device and the Outer layer of encryption. When an Outer VPN Gateway is used as part of an EUD, there is no requirement to utilize a Government RD (see Appendix D). The VPN Gateway included as part of the EUD must be physically connected to the component which provides the Inner layer of encryption. VPN Gateways included as part of a EUD are selected from the *IPsec VPN Gateway* section of the CSfC Components List.

When an Outer VPN Gateway is included as part of an EUD, it provides configuration and enforcement of network packet handling rules for the Outer Layer of Encryption. The configuration settings of the Outer VPN Gateway may need to be updated when entering new environments (e.g. updating the Default Gateway).

6.1.2 Outer VPN Client

An Outer VPN Client can be utilized as the Outer VPN Component for MA EUDs. The purpose of the Outer VPN Client is to establish an IPsec tunnel to the Outer VPN Gateway of the MA Solution Infrastructure. The tunnel can be configured to automatically be established as part of the EUD's power-on process. A combination of the VPN Client and the Operating System on which it is installed is responsible for providing configuration and enforcement of network packet handling rules for the Outer layer of encryption. The Outer VPN Client is selected from the *IPSec VPN Client* section of the CSfC Components list. The VPN Client is installed on the computing device selected from the *Mobile Platform* section of the CSfC Components List.

6.2 Virtual private Network (VPN) End User Device (EUD)

VPN EUDs utilize IPsec using a VPN Client to provide the Inner layer of encryption. The purpose of the Inner VPN Client is to establish an IPsec tunnel to the Inner VPN Gateway of the MA Solution Infrastructure. The tunnel can be configured to automatically be established as part of the EUD's power-on process, following establishment of the Outer VPN tunnel. Once the Inner VPN Client establishes the

inner IPsec tunnel, any application installed on the computing device can send and receive classified data with the Enterprise/Red network.

The private keys and certificates utilized for the authentication of the Inner VPN Component are considered CUI and must be at a minimum be protected by enabling the native platform DAR protection. Customers deploying Mobile Access Solutions in high-threat environments may also choose to implement controls to mitigate against tampering attacks.

Appendix D provides more detail on the allowable configuration of VPN EUDs.

6.2.1 Inner VPN Client on Computing Device

A VPN Client can be utilized as the Inner VPN Component for VPN EUDs. The purpose of the Inner VPN Client is to establish an IPsec tunnel to the Inner VPN Gateway of the MA Solution Infrastructure. The tunnel can be configured to automatically be established as part of the EUD's power-on process. A combination of the VPN Client and the Operating System on which it is installed is responsible for providing configuration and enforcement of network packet handling rules for the Inner layer of encryption. The Inner VPN Client is selected from the *IPSec VPN Client* section of the CSfC Components list. The VPN Client is installed on the computing device selected from the *Mobile Platform* section of the CSfC Components List.

Virtualization must be utilized when an Outer VPN Client and Inner VPN Client both reside on the same computing device. The virtualization ensures that two separate IP stacks are utilized. The MA CP allows for Type 1 or Type 2 Hypervisors to be utilized to provide logically separated operating systems, each with their own IP stack.

6.3 Transport Layer Security (TLS) End User Device (EUD)

TLS EUDs utilize TLS clients or SRTP clients to provide the Inner layer of encryption. The Inner layer of TLS or SRTP is implemented by TLS clients and SRTP clients provided by individual applications installed on the computing device. Each application which sends and receives data to the Enterprise/Red network must be selected and configured in accordance with the requirements of the CP. Each application then terminates the Inner layer of encryption to TLS-Protected Servers and SRTP Endpoints within the MA Solution Infrastructure.

The private keys and certificates utilized for user authentication of the Inner TLS and SRTP clients are determined by the AO. If the private keys and certificates are considered CUI then the EUD component must, at a minimum, implement the native platform encryption. If the private keys and certificates are considered to be classified, then the EUD must be treated as classified at all times or implement a NSA-Approved DAR Solution (see Section 4.2.1). Customers deploying MA Solutions in high threat environments may also choose to implement controls to mitigate against tampering attacks.

TLS EUDs must use either a Government RD or Outer VPN Gateway to connect to the Black network, except for the use cases defined in Section 4.1.3. Appendix D provides more detail on the allowable configuration of TLS EUDs.

6.3.1 TLS CLIENT

Applications with a TLS client can be installed on the computing device and utilized for the Inner layer of TLS encryption. On TLS EUDs every application which sends or receives data through the Outer VPN Component must be configured in accordance with the requirements of this CP. For example, if a Voice Application, Web Browser, MDM Agent, and Email Client are installed on the computing device each application is configured to establish a TLS session to the TLS-Protected Server in the MA Solution Infrastructure. In some instances an application may perform both TLS and SRTP encryption. Those applications must be configured to meet requirements for both TLS clients and SRTP clients.

TLS clients utilize certificates for mutual authenticate with the TLS-Protected Server. In most cases, the TLS-client utilizes a user certificate for authentication to the TLS-Protected Server. User certificates are issued by the same PKI that issues certificates to TLS Protected Servers (e.g. customer enterprise PKI), which may be different than the Inner CA. Alternatively, the TLS client can utilize a device certificate for authentication followed by user authentication (e.g. username and password, token, smartcard, etc). A combination of the TLS Client and Computing Device Operating System is responsible for providing configuration and enforcement of network packet handling rules for the Inner layer of encryption.

6.3.2 SRTP CLIENT

Applications with a SRTP client can be installed on the computing device and utilized for the inner layer of SRTP encryption. If multiple SRTP clients are installed on the TLS EUD, then each must be configured in accordance with the requirements of this CP. SRTP Clients are generally used to encrypt real time traffic, such as voice or video. In some instances, an application may perform both TLS and SRTP encryption. Those applications must be configured to meet requirements for both TLS clients and SRTP clients.

SRTP clients utilize certificates for mutual authentication. In most cases, the SRTP-client utilizes a user certificate for authentication. User certificates are issued by the same PKI that issues certificates to TLS Protected Servers (e.g. customer enterprise PKI), which may be different than the Inner CA. Alternatively, the SRTP client can utilize a device certificate for authentication followed by user authentication (e.g. username and password, token, smartcard, etc.). A combination of the SRTP Client and Computing Device Operating System is responsible for providing configuration and enforcement of network packet handling rules for the Inner layer of encryption.

The Inner layer of SRTP encryption can terminate either at a SRTP Endpoint within the MASolution Infrastructure or on another EUD. In either case, all SRTP encrypted traffic must go through the Outer VPN Component prior to being transmitted on the Black network.

7 MOBILE ACCESS CONFIGURATION AND MANAGEMENT

The Mobile Access CP includes design details for the provisioning and management of Solution Components. The following sections describe the design in detail and Section 13 articulates the specific requirements which must be met to comply with the MA CP.

7.1 SOLUTION INFRASTRUCTURE COMPONENT PROVISIONING

Provisioning is an out-of-band process performed in a physically secured area (e.g. the enterprise within the Red network), through which Mobile Access Solution Infrastructure Components are configured and initialized before their first use. During the provisioning process, the Security Administrator configures the Outer VPN Gateway, Gray Management Services, Inner Encryption Components, and Red Management Services in accordance with the requirements of this CP. During provisioning, the Solution Infrastructure Outer VPN Gateways and Inner Encryption components generate a public/private key pair and output the public key in a Certificate Signing Request (CSR). The Security Administrator delivers the Outer VPN Gateways CSR to the Outer CA and the Inner Encryption Components CSR to the Inner CA. The appropriate CA processes the CSR for each encryption component and returns a signed X.509v3 certificate for each encryption component. The Security Administrator then installs the unique signed certificate and the certificate of the Trust Anchor.

7.2 EUD PROVISIONING

Provisioning is an out-of-band process performed in a physically secured area (e.g. the enterprise within the Red network), through which MA EUDs are initialized before their first use. During the provisioning process, the Security Administrator loads and configures the required software for the EUD. The Security Administrator also instructs the EUD to generate the requisite public/private key pairs for the EUD's Outer VPN Component and Inner Encryption Component, and to output the public keys in a specified CSR format for delivery to the Outer CA and Inner CA, respectively. For TLS EUDs that require an enterprise user certificate, the CSR is delivered to the CA in the customer's organization that has the authority to issue enterprise user certificates. This CA may not be the same as the Inner CA. If the EUD cannot generate its own key pairs or CSRs, then a dedicated management workstation is required to generate the key pairs for the EUD and construct the CSRs for delivery to the Outer CA and Inner CA. The CAs process the CSRs and return signed certificates to the Security Administrator, who installs the certificates onto the EUD. If required, the Security Administrator also installs the private keys onto the EUD. The Security Administrator then finalizes the security configuration of the EUD before it used for the first time.

If the MA solution owner is unable to remotely manage EUDs, the EUDs must be periodically re-provisioned in order to receive software and configuration updates. Re-provisioning consists of revoking the EUD's existing certificates and provisioning the EUD using a trusted baseline configuration that does not make use of any retained data originally stored on the EUD (e.g. factory reset and provision as a new device). This CP does not impose a particular frequency with which re-provisioning must take place,

although without remote management of EUDs, re-provisioning is the only means of applying security-critical patches to EUDs in accordance with requirement MA-GD-26.

Due to the time and effort needed to re-provision EUDs, it is preferable to remotely manage them when possible. With remote management capabilities, updated software and configuration data can be provided from a central management site through the MA solution to the EUD, after the EUD establishes the two MA solution tunnels (see Section 13.11).

7.3 Administration of Mobile Access Components

Each component in the solution has one or more Administration Workstations that are responsible for maintaining, monitoring, and controlling all security functions for that component. Throughout this document, these workstations are referred to as Administration Workstations. It should be understood that all of the required administrative functionality does not need to be present in each individual Workstation, but the entire set of Administration Workstations must collectively meet administrative functionality requirements.

The Administration Workstation is used for configuration review and management. Implementations will employ an SIEM in the Gray Management Services for log management of Gray Infrastructure Components except where AOs utilize one-way taps to move Gray network log data to a Red SIEM. Given the architecture of the solution, each layer has its own distinct administration LAN or VLAN: the Inner Encryption Components are managed from the Red Management Services, and the Outer VPN Gateway and supporting components are managed from the Gray Management Services. The Gray Administration Workstation, along with all Gray Management Services, is physically connected to the Gray firewall. In this manner, the Gray firewall maintains separate ACLs to permit Management Traffic to/from Gray Management Services, but prohibits such traffic from all other components. This architecture provides the separation necessary for two independent layers of protection.

Administration Workstations will be dedicated for the purposes given in the CP. For example, Administration Workstations are not to be used as the registration authority for the CA, a SIEM, or as a general user workstation for performing any functions besides management of the solution. Administration Workstations cannot be used as an enrollment workstation or provisioning workstation.

Management of all Mobile Access Solution components is always encrypted to protect confidentially and integrity, except in the case where components are locally managed through a direct physical connection (e.g. serial cable from Gray Administration Workstation to Outer VPN Gateway). Management traffic must be encrypted with SSHv2, TLS, or IPsec. Additionally, when managing components over the Black Network the SSHv2, TLS, or IPsec protocols must be configured utilizing the appropriate Suite B Algorithms. A similar requirement is not imposed if the Mobile Access Solution Infrastructure components are being managed from the same LAN or VLAN. For example, a Gray Administration Workstation residing in the Gray Management Services at the same site as the Outer VPN Gateway need not use Suite B algorithms since this traffic does not traverse an untrusted network.

In most cases, Mobile Platforms are managed over the Black network utilizing the Outer layer of IPsec and a MDM Server selected from the CSfC Components List. When an MDM Server is used to manage TLS EUDs, the MDM Server is considered a TLS-Protected Server and the MDM agent is considered a TLS Client. As a result, the MDM Server must be placed either at Inner Encryption Component Option 1 or Inner Encryption Component Option 2 as denoted in Figure 4Figure 3. As a TLS-Protected Server, the MDM Server must be configured to establish a session with the MDM Agent in accordance with the requirements in Table 14. Although not mandatory, the use of an MDM enables organizations to dynamically change policies enforced on the phone, allowing more flexibility then requiring phones to be re-provisioned. Additionally, there are several security advantages by using an MDM including the ability to perform a remote wipe of the EUD.

7.4 EUDs for Differing Classification Domains

As specified in this CP, an EUD is only authorized to communicate to Enterprise/Red networks operating at the same classification level. However, it does not preclude the possibility that an approved Cross Domain Solution (CDS) can be used within an infrastructure to provide cross domain transfer of data between EUDs operating at differing classification levels. Neither does it preclude the use of an EUD as an access CDS for multiple enclaves operating at differing classification levels if approved through the appropriate CDS approval process.

The requirements for a CDS capable of providing separation between enclaves of two or more classification levels are outside the scope of this CP. If developing a Mobile Access solution with a CDS capability, the solution must register against this CP and utilize the appropriate CDS approval processes.

8 CONTINUOUS MONITORING

The Mobile Access CP allows customers to utilize EUDs from physical environments which do not necessarily reside within a government secure facility. With the increase in accessibility also comes a need to continuously monitor network traffic and system log data within the solution infrastructure. This monitoring allows customers to detect, react, and report to any attacks which occur on their solution. This continuous monitoring also enables the detection of any configuration errors to Solution Infrastructure Components.

At a minimum, the CP requires an Auditor to review alerts, events, and logs on a weekly basis. This minimum review period allows customers in Tactical Environments to implement solutions where it may not be feasible to perform real-time monitoring. Operational and Strategic implementations of the Mobile Access CP should review alerts, events, and logs on a much more frequent period and in many cases may leverage Operations Centers to perform 24/7 monitoring of the solution.

8.1 Monitoring Network Traffic

The MA CP requires monitoring network traffic in at least one of three areas within the Solution Infrastructure. Network traffic can be monitored using an IDS; however, it is preferable to utilize an IPS

to enable real-time responses. While it is only required to monitor one of the three locations, customers monitoring all three points have the best visibility enabling detection of malicious activity or misconfiguration of components.

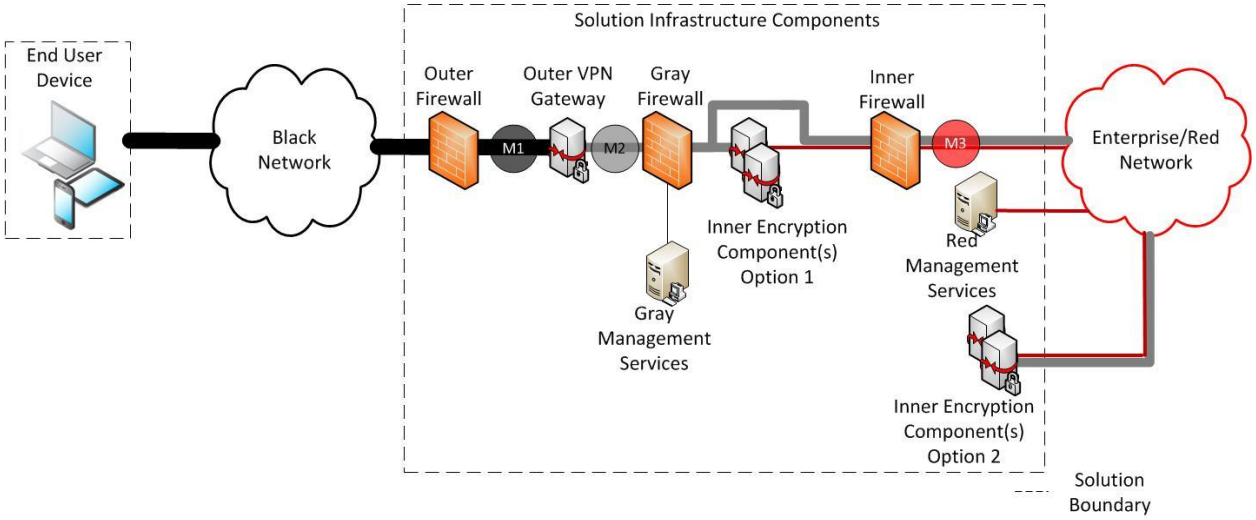

Figure 6. MA Solution Continuous Monitoring Points

Figure 6 depicts the three locations that customers can select to implement network monitoring capabilities. There are several alternatives for deploying the IDS at one or all of the Monitoring Points (M1, M2, and/or M3). Intrusion Detection Systems can ingest traffic from network taps, span ports, or in line with the solution. Similarly, an IPS can be placed either inline or in promiscuous mode. When operating in promiscuous mode, the IPS analyzes traffic at M1, M2, or M3 and issues commands to the Outer firewall, Gray firewall, or Inner firewall to block traffic flows. The following paragraphs define each of the three Monitoring Points. These descriptions detail the analysis and alerts which would be generated by the IDS. If a customer decides to implement an IPS, then it should be configured to block that traffic flow and also send an alert.

Monitoring Point 1 (M1): Located between the Outer firewall and Outer VPN Gateway. At a minimum, a M1 IDS is configured to send alert upon detection of any traffic which should have been blocked by the Outer firewall or Outer VPN Gateway. These alerts indicate a failure of the filtering or encryption functions by one of the two components and are either indicative of an improper configuration or a potential compromise. Normal traffic at M1 is very well-defined (IPsec and limited number of AO approved control plane protocols) and, as a result, will generate very few false positives. Since nearly all traffic traversing M1 is encrypted with IPsec, the IDS is limited to analyzing IP addresses, ports, protocols, and net flow data. Management of a M1 IDS occurs from a Black network.

Monitoring Point 2 (M2): Located between the Outer VPN Gateway and Gray firewall. At a minimum, a M2 IDS is configured to send an alert upon detection of any traffic which should have been blocked by the Outer VPN Gateway or Gray firewall. These alerts indicate a failure of the filtering functions by one

of the two components and are either indicative of an improper configuration or a potential compromise. Normal traffic at M2 is not as well defined as that of M1, but includes IPsec, data plane traffic encrypted with TLS or SRTP, control plane traffic, and management traffic. It is important that customers understand what ports and protocols are utilized by each of the Inner Encryption Components to ensure that firewall filters are properly configured and Intrusion Detection Systems are well tuned. Nearly all traffic traversing M2 is encrypted either with IPsec, TLS, SRTP, or SSHv2 which prevents the ability to perform deep packet inspection. Management of a M2 IDS occurs from the Gray Management Services.

Monitoring Point 3 (M3): Located between the Inner firewall and Enterprise/Red network. At a minimum, a M3 IDS is configured to send an alert upon detection of any traffic which should have been blocked by the Inner firewall. These alerts indicate a failure of the filtering function of the Inner firewall. Of the three monitoring points, M3 is the most difficult to define a normal baseline, but in many implementations, monitoring at M3 allows for deep packet inspection since traffic is not necessarily encrypted. If the Mobile Access Solution Infrastructure supports TLS EUDs that terminate within the Enterprise/Red network, then data traversing M3 will still have a single layer of encryption. Management of the M3 IDS occurs from the Red Management Services.

Monitoring Multiple Points: Although the MA CP only requires monitoring of one out of the three points, customers are encouraged to monitor all three locations. To ensure that no bypass of the Outer or Inner Encryption Components occurs, customers can implement three IDS(s)/IPS(s) located in the Black, Gray, and Red networks. Implementation of three separate components to monitor each point ensures that malicious traffic cannot inadvertently be transferred to the Enterprise/Red network, but it also increases cost and complexity for managing the solution. This approach also prevents correlation of data as it traverses throughout the solution.

Alternatively, in order to allow correlation of data at multiple points the MA CP allows a one-way tap located at M2 to feed the IDS located in an enclave of the Red Network that is isolated from the Enterprise/Red network. The one-way tap utilized must physically only allow data flow from M2 to the Enterprise/Red network. Additionally, the selected one-way tap must be approved by the AO. Similarly, the CP also permits an AO-approved one-way tap located at M1 to feed the IDS located in the Enterprise/Red network. Movement of network traffic from M3 to the Gray or Black network is explicitly prohibited. Additionally, movement of Network Traffic from M2 to the Black network is explicitly prohibited. Prior to implementing one-way taps as part of the Mobile Access Solution, AOs need to be aware of the Residual Risks associated with transferring data from Black and Gray networks to a Red network of a higher classification.

8.2 Monitoring Log Data

The Mobile Access CP requires the implementation of a SIEM component within the Gray Management Services (except in instances where an AO utilizes one-way taps to feed Gray Log data to a Red SIEM).

The Gray SIEM collects, aggregates, correlates, and analyzes log data from Gray Management Components. The SIEM also provides alerts to auditors when anomalous behavior is detected.

The Gray SIEM collects logs from the Outer VPN Gateway, Gray firewall, and any components located within the Gray Management Services. The Gray SIEM is not permitted to collect logs from the Outer firewall, Inner Encryption Components, or Inner firewall unless utilized in conjunction with AO-approved one-way taps. To protect the integrity of the data, all logs sent to the SIEM should be encrypted with TLS, SSHv2, or IPsec. At a minimum the SIEM is configured to send alerts upon receiving a log entry for blocked packets from the Outer VPN Gateway or Gray firewall. Packets blocked by the Outer VPN Gateway either indicate a failure of the Outer firewall or a failure of the Gray firewall. Similarly, packets blocked by the Gray firewall either indicate a failure of the Outer VPN Gateway, Inner Encryption Components, or Inner firewall.

In order to allow correlation of data from both Gray and Red components the MA CP allows a one-way tap located in the Gray Network to feed Gray Log Data to a Red SIEM located in an enclave of the Red Network that is isolated from the Enterprise/Red network. The one-way tap utilized must physically only allow log data to flow from Gray Components to the Enterprise/Red network. Additionally, the selected one-way tap must be approved by the AO. Similarly, the CP permits an AO-approved one way tap located in the Black Network to feed Black Component Log Data (i.e. Outer firewall) to an enclave of the Red Network that is isolated from Enterprise/Red network.

9 KEY MANAGEMENT

MA solutions utilize asymmetric algorithms (as defined in table 9 - 11) and X.509 v3 certificates for Component authentication to establish the outer and inner encryption tunnels. Each MA solution Component contains a private authentication key and a corresponding public certificate issued by an authorized CA. In addition, a Trusted CA certificate is installed as well as any other CA signing certificates that chain to the Trusted CA, so that a trusted certificate chain is established between the Component certificate and the Trusted CA certificate. Each MA Solution Infrastructure component should also contain the required CRLs to support revocation status checking of Component certificates. If CRLs are not used, other mechanisms can be implemented (e.g. whitelists) in MA solution infrastructure components.

It is preferable for the authentication keys (public/private key pair) to be generated on the security Component, where the private keys are never exported out of the Component. If the Component cannot generate its own key pair, a dedicated management workstation is required to generate the key pair for the Component. The public keys are sent in certificate requests to the Outer and Inner CAs that create and sign authentication certificates containing the public keys. If the request is for a user certificate, the request is delivered to the CA in the customer's organization that has the authority to issue enterprise user certificates. This CA may not be the same as the Inner CA. The authentication certificates are delivered to, and installed on the security Components during provisioning, along with

the private keys if they were not generated on the Component. The CAs also issue signed CRLs to provide revocation status information for the certificates issued by the CAs. CRLs are transferred to CDPs or OCSP Responders as discussed in Section 9.1, where the CRLs or Certificate Statuses are made available to MA Solution Infrastructure Components.

To provide confidentiality services within MA solutions, the Components utilize key agreement protocols (such as Elliptive Curve Diffie-Hellman(ECDH)) to generate ephemeral encryption keys. The use of ephemeral encryption keys is not part of key management discussed in this section, as CAs are not required in issuing and managing these keys.

The CAs that issue authentication certificates to MA solution Components operate either as Enterprise CAs (e.g. DoD PKI, KMI, and Agency PKI) or locally run CAs. Existing Enterprise CAs should be used whenever possible, as the advantages for using these CAs outweigh those associated with locally run CAs. Enterprise CAs have established operations, as well as Certificate Policies and Certification Practices Statements (CPSs) that customer organizations can leverage for their MA solution. These Enterprise CAs operate at Federal Department (e.g. DoD PKI, KMI) and Agency levels, and offer wide-scale interoperability across MA solutions (i.e., the certificate policies and their registered policy Object Identifiers (OIDs) are widely accepted across the Federal Department or Agency). When an Enterprise Root CA is utilized, the MA CP requires that at least two existing Subordinate CA's are used to issue certificates. One Subordinate CA issues certificates to Outer Encryption Components (known as the Outer CA) and the other CA is utilized to issue certificates to Inner Encryption Components (known as the Inner CA). To ensure that the same certificate cannot be used for authenticating both the outer and inner tunnels, the Outer CA and Inner CA are used as trust anchors to validate the outer tunnel and inner tunnel authentication certificates, respectively.

For MA solutions requiring interoperability across a Federal Department, the Department-level Enterprise CAs should be leveraged. Examples of Department-level Enterprise CAs include the DoD PKI; the NSA Key Management Infrastructure (KMI); the National Security Systems (NSS) PKI; the Intelligence Community (IC) PKI; the Department of Homeland Security (DHS) PKI; and the Department of Energy (DoE) PKI. Enterprises like this leverage Department-level Trusted CAs which reside under the same Root CA. Trusted CAs like this can be used as trust anchors in multiple MA solutions throughout a Federal Department, thereby providing certificate trust interoperability across those MA solutions. In addition, certificates issued by Department-level Enterprise CAs may assert registered policy OIDs that are acceptable for use through the Federal Department. A user with a MA EUD provisioned with certificates from a Department-level Enterprise CA could possibly use their EUD in many different MA solutions deployed throughout a Federal Department.

Similarly, MA solutions requiring interoperability across a Federal Agency should leverage Agency-level Enterprise CAs. Agency-level Enterprise CAs issue certificates only to Agency personnel and Non-Person Entities (NPEs). Enterprises like this leverage Agency-level Trusted CAs which resides under the same Root CA. Trusted CAs like this can be used as trust anchors in multiple MA solutions throughout that

Agency. Furthermore, certificates issued by Agency-level Enterprise CAs may assert registered policy OIDs that are acceptable for use through the Federal Agency. A user with a MA EUD provisioned with certificates from an Agency-level Enterprise CA could possibly use their EUD in different MA solutions deployed throughout that Federal Agency.

For both types of Enterprise CAs described above, an MA solution owner could deploy and operate independent Subordinate CAs that are issued certificates by a higher-level Enterprise CA. The benefit of this configuration is that it allows tailoring of the Subordinate CA operations to the local environment without losing the interoperability benefits gained by leveraging Enterprise CAs. However, the MA solution owner is responsible for defining and implementing CPSs for the Subordinate CAs that are approved by the Enterprise CA policy authorities.

Finally, MA solutions requiring minimal or no interoperability can deploy and operate their own locally run CAs that are independent of any Enterprise CAs. In this configuration, certificate policy and interoperability is constrained to the specific MA solution. Furthermore, the MA solution owner is required to develop and maintain CPSs that detail the operational procedures for the locally run CAs. In addition, the customer may need to develop and maintain a higher-level Certificate Policy if one does not already exist.[1] Table 4 summarizes the differences between Enterprise and ocally run CAs.

Table 3. Certificate Authority Deployment Options

CA Type	Certificate Policy	Interoperability	Operations
Department-level Enterprise	Owned and managed at the Department level (e.g. DoD PKI, NSA KMI, NSS PKI, IC PKI, DHS PKI, DoE PKI)	Department-wide	Performed by the enterprise
Agency-level Enterprise	Owned and managed at the Agency level	Agency-wide	Performed by the enterprise
Subordinate CA (Enterprise)	Owned and managed at the Department or Agency level	Department-wide or Agency-wide	Performed by the enterprise and the MA solution owner
Locally run (Non-Enterprise)	Owned and managed at the MA solution level	Constrained to the MA solution	Performed by the MA solution owner

In all CA configurations identified above, Outer CAs issue and manage authentication certificates for Outer VPN Components and Gray Management Service Components; Inner CAs, and optionally existing CAs that support enterprise services, issue and manage authentication certificate for Inner Encryption Components and Red Management Service Components. Outer CAs can be included as either part of

[1] CNSSP 25 is the governing policy for PKI solutions in support of Secret MA solutions. For MA solutions that are higher than Secret, the MA solution owner is required to develop a Certificate Policy that is approved by the local Approving Official (AO).

the Gray network or Red network. Inner CAs, including existing enterprise CAs, can only be located in the Red network.

To assist the CAs in their operations, the CAs may communicate with management services (e.g., Device Managers (DMs)) deployed in the corresponding network to support enrollment and life-cycle certificate management for MA Solution Components. Outer and Inner CAs in the Red network are limited to directly communicating with Red Management Services. Outer CAs in the Gray network are limited to directly communicating with Gray Management Services. When the CA is not located in the same network as the required management services, an AO-approved Cross Domain Solution may be utilized allowing indirect communication (for example Certificate Enrollment). The Red and Gray Management Services enable the certificate request/response process between a MA Solution Component and a CA. This CP recommends provisioning of MA Solution Components in the Red network, and that all enrollment and life-cycle certificate management be performed in accordance with the applicable Certification Practices Statements (CPSs).

This solution utilizes device authentication certificates and, in some instances, user authentication certificates. Device certificates and private keys used in the solution are considered CUI (unless determined to be higher by the AO) because they are only used for mutual authentication, not for traffic encryption or granting access to classified data. User private keys are classified to the level determined by the AO. Often user private keys are treated as classified to the level of the Enterprise/Red network. While the Capability Package enables AOs to define the classification level of User and Device private keys, the allowable options for use and handling of EUDs is dependent on that classification. If any of the private keys stored on an EUD are considered classified, then the solution must be treated as classified at all times or implement a NSA approved DAR Solution. Conversely, if the private keys stored on the EUD are determined to be CUI then the EUD can also be utilized as a Thin EUD (see Section 4.2.1).

The MA solution described here requires certificates to establish the secure tunnels between Components. Without certificates, the network cannot function. Thus, an out-of-band method must be used to issue the initial certificates to the Components. Subsequent rekeying, however, should take place over the network through this solution prior to the current key's expiration. The key validity period for certificates issued by locally run CAs cannot exceed 14 months, while the key validity period for certificates issued by an Enterprise CA are inherited from the Enterprise CA certificate policy. Updates to CRLs are distributed to Gateways within 24 hours of CRL issuance.

9.1 Distribution Of Certificate Revocation Lists

Certificate-based mutual authentication is required between MA solution components in order to establish the outer and inner encryption tunnels, as well as the encryption tunnels (i.e. device management tunnels) that are used to securely administer and manage the configurations of the outer and inner security infrastructure boundary devices. Part of the mutual authentication process includes checking the revocation status of the Component certificates to ensure they are not revoked prior to

establishing the outer and inner encryption tunnels. Certificate Revocation Lists (CRLs) are used by CAs to convey the revocation status of certificates issued by those CAs, and those CRLs need to be made available to the MA solution components.

A CDP is a web server whose sole function is to provide external distribution of, and access to CRLs issued by CAs. CDPs do not serve any other content, and, in particular, do not host any dynamically generated content. CDPs also do not provide any other services other than the distribution of CRLs. CDPs are optional in an MA solution, and they can exist in the Gray or Red networks. The Outer VPN Gateway in the Solution Infrastructure accesses an Outer CDP, located in the Gray network, to obtain CRLs and check revocation status of EUD Outer VPN Components prior to establishing the outer encryption tunnel. Furthermore, a CDP operating in the Gray network can be accessed by Gray Management Service Components to obtain CRLs and check the revocation status of the Outer VPN Gateway's certificate prior to establishing a device management tunnel with the Outer VPN Gateway. Additionally, the Mobile Access CP also allows for an Inner CDP to be stood up in the Gray Management Services. Placing an Inner CDP in the Gray Management services allows EUDs to check the certificate status of the Inner Encryption component prior to establishing a tunnel. To utilize an Inner CDP in the Gray Management Services, an AO must determine that CRLs generated by the Inner CA are unclassified. These CRLs must also be moved from the Enterprise/Red network to the Gray Management Services using an AO approved method (e.g. Cross Domain Solution).

Solution Infrastructure Inner Encryption Components access an Inner CDP, located in the Enterprise/Red network, to obtain CRLs and check revocation status of EUD Inner Encryption Components prior to establishing the inner encryption tunnel. Likewise, a CDP operating in the Red network can be accessed by Red Management Service Components to obtain CRLs and check the revocation status of the Inner Encryption Component's certificate prior to establishing a device management tunnel with the Inner Encryption Component.

An Outer CDP and an Outer CA may reside on the same or different networks. For example, the Outer CA may be operated in the Red network, while the Outer CDP operates in the Gray network. If they reside on different networks, a one-way transfer mechanism is required to periodically distribute the current CRL from the CA to the CDP. The details and procedures of the one-way transfer mechanism are left to a solution's Authorizing Official (AO).

As CRLs are digitally signed objects that contain minimally identifying information about MA solution components, there are few concerns with the confidentiality of CRLs. Therefore, CRLs can be downloaded by MA solution components over unencrypted Hypertext Transfer Protocol (HTTP). Furthermore, a CRL's integrity is protected by the digital signature of the CA that issued it, and additional integrity protection during CRL download is not required. Additionally, placement of CDPs on the Gray network for the Outer VPN Gateway and Enterprise/Red network for Inner Encryption Components reduces the exposure to external threat actors.

Use of HTTPS for CRL downloading is discouraged, as it introduces a circular dependency between the CDP and the MA solution Component attempting to download the CRL. The MA solution Component would need a CRL to determine whether the CDP's certificate is revoked before establishing an HTTPS connection to the CDP. However, the CDP cannot deliver the CRL to the MA solution Component until the MA solution Component authenticates the CDP by validating its certificate. (Note: Distributing CRLs via HTTP follows the recommendation in Internet Engineering Task Force (IETF) Request for Comments (RFC) 5280 not to use HTTPS to distribute CRLs.)

To provide redundancy and ensure that current CRLs are always made available to MA solution Components, multiple Outer and Inner CDPs may be deployed. The use of multiple CDPs is left to the discretion of the MA solution owner. Furthermore, CDPs may host delta CRLs in addition to complete CRLs. In large MA solutions, the use of delta CRLs can reduce the amount of network traffic needed to distribute updates to CRLs. A CA's Certificate Policy will define whether the use of delta CRLs is permissible.

An OCSP Responder or white lists can be utilized in lieu of a CDP Server. An OCSP Responder located in the Gray network can provide Certificate Status information to the Outer VPN Gateway. Additionally, a OCSP Responder in the Enterprise/Red network can provide Certificate Status information to Inner Encryption Components.

10 THREATS

This section details how the required components work together to provide overall security in the solution. Section 4.2 shows the boundary of the MA solution for each high-level design covered by this CP.

An assessment of security was conducted on each of the high-level designs described in this CP while making no assumptions regarding use of specific products for any of the defined components. There are several different threats to consider when evaluating the risk of transporting data over secure or unsecure networks. By examining these threats, the organization can have a better understanding of the risks they are accepting by implementing the solution and how these risks affect the Confidentiality, Integrity, and Availability of the network, systems, and data. To obtain the classified risk assessment associated with this CP, please contact the NSA via your Client Advocate.

10.1 PASSIVE THREATS

This threat refers to internal or external actors attempting to gain information from the network without changing the state of the system. Threat actions include collecting or monitoring traffic (e.g. traffic analysis or sniffing the network) passing through a network in order to gain useful information through data analysis.

The security against a passive attack targeting the data in transit across the Black network is provided by the layered IPsec tunnels. To mitigate passive attacks, two layers of Suite B encryption, Advanced Encryption Standard (AES), are employed to provide confidentiality for the solution. Use of AES is approved to protect classified information, meeting IAD and CNSSP-15 guidance for adequate confidentiality. The two Encryption Components that are used to set up the tunnels must be independent in a number of ways (see Section 12). Due to this independence, the adversary should not be able to exploit a single cryptographic implementation to compromise both tunnels.

The use of EUDs to access classified information outside of a secure physical environment opens the possibility that an attacker with physical access to the EUD's immediate environment could use surveillance techniques to obtain classified information without the user's knowledge while the EUD is in use. The organization-defined user agreement tells users of EUDs what measures they must follow when using and storing the EUD to mitigate this threat.

10.2 External (Active) Threats

This threat refers to outsiders gaining unauthorized access to a system or network, exfiltration of sensitive Red network data, or degradation of availability of the system or network. Threat actions include introducing viruses, malware, or worms with the intention to compromise the network or exfiltrate data, or to analyze the design of the network or system for future attacks. Adversaries could gain access to a VPN Gateway or EUD, and then exploit or compromise other devices on the network. DoS or Distributed DoS (DDoS) attacks compromise availability of the system, degrading/disrupting secure communication across a Black network. Further external threat actions would include social engineering attacks to assist attackers with gaining additional access to a network for the purpose of compromising a system or network, traffic injection or modification attacks, or replay attacks.

10.2.1 Rogue Traffic

One method for detecting rogue traffic from an external attack as it attempts to pass through one or both Encryption Components is by having the port filtering native to each VPN Gateway enabled and configured to audit and log any traffic that is not one of the formats described in the configuration (see Section 13.9). It is required that the port filtering be set up to block the following: 1) any traffic not coming from or going to an IP address on the network at the other site, 2) traffic not contained in IP packets other than control plane protocols needed for network operation and approved by AO policy, and 3) traffic going to unexpected ports. This will allow the Auditor(s) and/or the Security Administrator(s) to detect whether the Outer VPN Gateway has been breached, thus providing an early warning of a potential intrusion. It will also provide detection of misconfigured Outer VPN Gateways.

Another method for detecting a potential intrusion into the solution is requiring automated configuration change detection on Red and Gray Management networks to ensure that VPN Gateway configurations are not changed without the knowledge of Auditors and Security Administrators.

Auditors also ensure through the audit logs that all configuration changes are valid. This will counter attacks that take advantage of VPN Gateway misconfigurations.

End User Devices (EUDs) are protected from rogue traffic through the use of traffic filtering rules configured on their interfaces connected to Black networks to drop any traffic not necessary for connecting to the necessary Outer VPN Gateway.

CRL Distribution Points (CDPs) are protected from rogue traffic by implementing port filtering on the server. Rogue traffic to CDPs can be further mitigated by implementing a firewall or other packet filtering device between the CDP and the rest of the network.

10.2.2 Malware and Untrusted Updates

Administration Workstations and locally run CAs for Inner Tunnel Components shall be distinct and physically separate from the Administration Workstations and locally run CAs for Outer Tunnel Components. This separation minimizes the potential for malware on a single device to impact components supporting both Inner and Outer MA solution tunnels.

Each individual component of this solution has the capability to perform trusted updates through verification of a signature or hash to ensure that the update is from a reliable source, such as signed by the vendor. This mitigates threats of malicious users trying to push updates or code patches that affect the security of the component (and therefore system). The source of all updates and patches should be verified before installation occurs.

10.2.3 Denial of Service

Denial of Service (DoS) attack risks cannot be completely mitigated. MA solutions in compliance with this CP requires that the Outer firewall drop all packets that are not Internet Key Exchange (IKE), Encapsulating Security Payload (ESP), or other approved protocols on the appropriate interfaces, which significantly reduces the potential for flooding attacks. For customers that require more protection against these attacks, one option is the use of a multiple Outer firewalls between the Outer VPN Gateway and Black networks to filter and load balance traffic before it reaches the Outer VPN Gateway. Another option for customers requiring more protection is to add additional filtering based on specifics like known network IP addresses to filter traffic from devices not included in this solution, although the feasibility of doing so for EUDs is limited. Other mitigations are acceptable and up to the AO to approve their use.

A single encryption component failure is likely to result in a DoS condition. One assumption underlying this solution is that high assurance of availability is not required. If availability is critical for the customer both network redundancy and instituting DoS response procedures when loss of availability is detected can provide further protection against DoS attacks.

10.2.4 Social Engineering

It is the responsibility of the customer to define the appropriate policies and training necessary to protect against Social Engineering attacks. In addition, these types of attacks generally take advantage of other attacks detailed in this section and are already discussed.

10.3 Insider Threats

This threat refers to an authorized or cleared person or group of people with physical or logical access to the network or system who may act maliciously or negligently, resulting in risk exposure for the organization. This threat could include poorly trained employees, curious employees, disgruntled employees, escorted personnel who gain access to the equipment, dishonest employees, or those that have the means and desire to gain escalated privileges on the network.

Threat actions include insertion or omission of data entries that result in a loss of data integrity, unintentional access to an unauthorized system or network, willingly changing the configuration of an EUD, unwillingly or unknowingly executing a virus or malware, intentionally exposing the network and systems to viruses or malware, cross-contaminating a system or network with data from a higher classification to a lower classification (e.g. Secret data to an Unclassified network or system), or malicious or unintentional exfiltration of classified data. Typically, the threat from insiders has the potential to cause the greatest harm to an organization, and insider attacks are also the hardest to monitor and track.

To mitigate insider threats, separation of roles within the solution is required (see Section 15). In addition, logging and auditing of security critical functionality (see Section 13.13) is required. Also, strong authentication of the Security Administrator and Auditor are required for access to ensure accountability of these individuals. Finally, outbound filters on Encryption Components, firewalls, and EUDs are configured to block traffic leaving the internal network that does not go through the Encryption tunnels. An IDS is also deployed on at a minimum the Black, Gray, or Red network to help identify unusual or suspicious traffic that could result from a failure, misconfiguration, or attack on Inner or Outer Encryption Components.

Additionally, organizations concerned about users misbehaving when connected remotely may wish to restrict the use of EUDs to those deemed sufficiently trustworthy.

10.4 Supply Chain Threats

A critical aspect of the U.S. Government's effectiveness is the dependability, trustworthiness, and availability of the Information and Communication Technology (ICT) components embedded in the systems and networks upon which the ability to perform U.S. Government missions rely. The supply chain for those ICT components are the underpinnings of those systems and networks and supply chain attacks are attempts to proactively compromise those underpinnings.

Unfortunately, the supplier cannot always provide guarantees of a safe delivery of a component; they are only able to provide assurances based on their reliance of established procedures and processes they have developed. In a single change of hands, the component may be introduced to potential threats and compromises on many levels.

The supply chain threat refers to an adversary gaining access to a vendor, retailer, reseller, or shipper and then attempting to insert or install a modification or a counterfeit piece of hardware into a component that is destined for a U.S. Government customer in an effort to gain information or cause operational issues. This threat also includes the installation of malicious software on components of the solution. This threat is difficult to identify, and is increasingly more difficult to prevent or protect against since vendors build products containing components manufactured by subcontractors. It is often difficult to determine where different pieces of components are built and installed within the supply chain.

Threat actions include manufacturing faulty or counterfeit parts of components that can be used to disrupt system or network performance, leaving open back doors in hardware that allow attackers easy ways to attack and evade monitoring, as well as easy ways to steal data or tamper with the integrity of existing/new data. Supply Chain attacks may occur during development and production, updates, distribution, shipping, at a warehouse, in storage, during operations, or disposal. For this reason, it is imperative that all components selected for use in CSfC solutions are subject to the applicable Supply Chain Risk Management (SCRM) process to reduce the risk of acquiring compromised components.

Each component that is selected from the CSfC Components List shall go through a Product Supply Chain Threat Assessment to determine the appropriate mitigations for the intended application of the component per the organization's AO-approved Product Supply Chain Threat Assessment process (see CNSSD 505 Supply Chain Risk Management (SCRM) for additional guidance). Even after selecting components from the CSfC Components List and utilizing a rigorous acquisition process, an AO must perform due diligence when integrating commercial components for mission operations.

Doctrinal requirements are placed on Product Selection, Implementers, and System Integrators of these solutions to minimize the threat of supply chain attacks (see sections 12, 14, and 15). To further mitigate Supply Chain Threats implementing organizations should utilize the following guidance.

- Establish an ICT SCRM program which conforms to applicable policy based on external and organizational requirements and constraints. The ICT SCRM program should be integrated into the organizational business and mission processes.
- Assess all aspects of the performance of potential vendors, not only the product quality, cost, and performance, but also supply chain risk factors of vendor selection. These risk factors include political ties to foreign governments, citizenship of employees, partner affiliations, employee clearance levels, and location of suppliers and sub-suppliers.

- Ensure that each component selected from the CSfC Components List go through a Product Supply Chain Threat Assessment to determine the appropriate mitigations for the intended application of the component (see CNSSD 505 Supply Chain Risk Management and Intelligence Community Directive (ICD) 731 Supply Chain Risk Management).

- Conduct a Criticality Analysis by which mission-critical functions and components are identified and prioritized with respect to improving acquirer practices (see Defense Acquisition Guidebook, Chapter 13).

Supply chain risk management is a critical consideration in acquiring commercial products. Even after selecting components from the CSfC Components List and utilizing a rigorous acquisition process an AO must do their due diligence as composed commercial products are integrated into mission operations.

10.5 Integrator Threats

This threat refers to an integrator who has unrestricted access to all components within the solution prior to the customer purchasing and implementing the solution within their system. This is different from a Supply Chain threat in that these integrators have access to all components to be used in the solution, rather than only those being procured from a particular vendor.

Threat actions could include installing or configuring components in a manner that places the organization at risk for attack or open to an unknown vulnerability that may not be detected through normal tests, scans, and security counter-measures.

In order to mitigate this threat, integrators are required to be cleared to the highest level of data protected by the MA solution. To further reduce the integrator threat, a customer may wish to use multiple integrators, such that no one integrator has access to all components of the solution. More information on the NSA's list of trusted integrators can be found on the NSA CSfC Website in the "Criteria For CSfC Integrators" section at this link: https://www.nsa.gov/ia/programs/csfc/index.shtml.

11 REQUIREMENTS OVERVIEW

The following five sections (Sections 12 through 16) specify requirements for implementations of MA solutions compliant with this CP. However, not all requirements in the following sections will apply to each compliant solution. Sections 11.1 and 11.2 describe how to determine which set of requirements applies to a particular solution.

11.1 Capabilities

This CP provides the flexibility needed to implement a variety of designs for the implementation of the MA solution. Although most requirements are applicable to all solutions, some requirements are only applicable to implementations whose high-level designs implement certain features. For example,

requirements dealing with TLS EUDs do not include requirements for an Inner VPN Client. Table 4 lists the capabilities covered by this CP and the designators used in the requirements tables to refer to each.

Table 4. Capability Designators

Capability	Designator	Description
TLS Solution	T	Requirement that applies to the MA Solution that connects to the Red network using IPsec as the Outer layer and TLS or SRTP as the inner layer, as described in Section 6.3
VPN Solution	V	Requirement that applies to the MA solution that connects to the Red network using two IPsec tunnels, as described in Section 6.2
TLS Infrastructure	TI	Requirement that applies specifically to the infrastructure associated with the TLS solution
VPN Infrastructure	VI	Requirement that applies specifically to the infrastructure associated with the VPN solution
TLS EUD	TE	Requirement that applies specifically to the EUD associated with the TLS solution
VPN EUD	VE	Requirement that applies specifically to the EUD associated with the VPN solution
All Solution Components	All	Requirement that applies to the EUD and to the Infrastructure, regardless if it is a VPN solution or a TLS solution
CDPs	C	Requirement that applies to the MA Solution that includes CDPs, as described in section 13.14.4

Any solution that follows this CP must implement each applicable capability for their solution (i.e. all VPN EUD (V), VPN Infrastructure (VI), and VPN Solution (V) requirements for a solution supporting only VPN EUDs), and may implement multiple capabilities. The "Capabilities" column in the requirements tables in Sections 12 through 16 identifies which capabilities the requirement applies to. A requirement is only applicable to a solution if the "Capabilities" column for that requirement lists one or more of the capabilities being implemented by the solution.

11.2 Threshold and Objective Requirements

In some cases, multiple versions of a requirement may exist in this CP. Such alternative versions of a requirement are designated as being either a Threshold requirement or an Objective requirement:

- A Threshold (T) requirement specifies a feature or function that provides the minimal acceptable capability for the security of the solution.
- An Objective (O) requirement specifies a feature or function that provides the preferred capability for the security of the solution.

In general, when separate Threshold and Objective versions of a requirement exist, the Objective requirement provides a higher degree of security for the solution than the corresponding Threshold

requirement. However, in these cases meeting the Objective requirement may not be feasible in some environments or may require components to implement features that are not yet widely available. Solution owners are encouraged to implement the Objective version of a requirement, but in cases where this is not feasible solution owners may implement the Threshold version of the requirement instead. These Threshold and Objective versions are mapped to each other in the "Alternatives" column. Objective requirements that have no related Threshold requirement are marked as "Optional' in the "Alternatives" column.

In most cases, there is no distinction between the Threshold and Objective versions of a requirement. In these cases, the "Threshold / Objective" column indicates that the Threshold equals the Objective (T=O). Such requirements must be implemented in order to comply with this CP, as long as the requirement is applicable per Section 11.1.

Requirements that are listed as Objective in this CP may become Threshold requirements in a future version of this CP. Solution owners are encouraged to implement Objective requirements where possible in order to facilitate compliance with future versions of this CP.

11.3 Requirements Designators

Each requirement defined in this CP has a unique identifier consisting of the prefix "MA," a digraph that groups related requirements together (e.g. KM), and a sequence number (11). Table 5 lists the digraphs used to group together related requirements and identifies the sections in which those requirement groups can be found.

Table 5. Requirement Digraphs

Digraph	Description	Section	Table
PS	Product Selection Requirements	Section 12	Table 6
SR	Overall Solution Requirements	Section 13.1	Table 7
CR	Configuration Requirements for Inner and Outer VPN Components	Section 13.3	Table 11
IR	Inner VPN Component Requirements	Section 13.4	Table 12
OR	Outer VPN Component Requirements	Section 13.5	Table 13
TE	TLS-Protected Server & SRTP Endpoint Requirements	Section 13.6	Table 14
RD	Retransmission Device Requirements	Section 13.7	Table 15
EU	End User Device Requirements	Section 13.8	Table 16
PF	Port Filtering Requirements for Solution Components	Section 13.9	Table 17
CM	Configuration Change Detection Requirements	Section 13.10	Table 18
DM	Device Management Requirements	Section 13.11	Table 19
MR	Continuous Monitoring Requirements	Section 13.12	Table 20
AU	Auditing Requirements	Section 13.13	Table 21

Digraph	Description	Section	Table
KM	Key Management Requirements	Section 13.14	Table 22, Table 23, Table 24, Table 25
GD	Requirements for the Use and Handling of Solutions	Section 14.1	Table 26
	Role-Based Personnel Requirements	Section 15	Table 28
RP	Incident Reporting Requirements	Section 14.2	Table 27
TR	Test Requirements	Section 16.1	Table 29

12 REQUIREMENTS FOR SELECTING COMPONENTS

In this section, a series of requirements are given for maximizing the independence between the components within the solution. This will increase the level of effort required to compromise this solution.

Table 6. Product Selection Requirements

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-PS-1	The products used for the Inner VPN Gateway shall be chosen from the list of IPsec VPN Gateways on the CSfC Components List.	VI	T=O	
MA-PS-2	The products used for any Outer VPN Gateway shall be chosen from the list of IPsec VPN Gateways on the CSfC Components List.	All	T=O	
MA-PS-3	The products used for any Inner VPN Client shall be chosen from the list of IPsec VPN Clients on the CSfC Components List.	VE	T=O	
MA-PS-4	The products used for any Outer VPN Client shall be chosen from the list of IPsec VPN Clients on the CSfC Components List.	TE, VE	T=O	
MA-PS-5	The products used for the Inner and Outer CAs shall either be chosen from the list of CAs on the CSfC Components List or the CAs shall be pre-existing Enterprise CAs (e.g. DoD PKI, IC PKI)..	VI, TI	T=O	
MA-PS-6	Products used for Mobile Platform EUDs shall be chosen from the list of Mobile Platforms on the CSfC Components List.	VE, TE	T=O	
MA-PS-7	Intrusion Prevention Systems (IPS) shall be chosen from the list of IPS on the CSfC Components List.	VI, TI	O	Optional
MA-PS-8	Products used for the TLS Client shall be chosen from the TLS Client sections (e.g. VoIP Applications, Email Clients, Web Browsers, etc.) of the CSfC Components List.	TE	T=O	

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-PS-9	Products used for the SRTP Client shall be chosen from the list of VoIP Applications on the CSfC Components List.	TE	T=O	
MA-PS-10	If the solution is using a TLS-Protected Server, it shall be chosen from the list of TLS-Protected Servers on the CSfC Components List.	TI	T=O	
MA-PS-11	If the solution is using an SIP Server, it shall be chosen from the list of SIP Servers on the CSfC Components List.	TI	T=O	
MA-PS-12	If the solution is using an SRTP Endpoint, it shall be chosen from the list of SRTP Endpoints on the CSfC Components List.	TI	T=O	
MA-PS-13	Products used for the Outer firewall, Gray firewall, and Inner firewall shall be chosen from the list of Stateful Traffic Filtering Firewalls (TFFW) on the CSfC Components List.	VI, TI	T=O	
MA-PS-14	If the solution is using a MDM, it shall be chosen from the list of MDMs on the CSfC Components List.	VI, TI	T=O	
MA-PS-15	Withdrawn			
MA-PS-16	The Outer VPN Gateway and Inner Encryption Endpoints shall either: • come from different manufacturers, where neither manufacturer is a subsidiary of the other; or • be different products from the same manufacturer, where NSA has determined that the products meet the CSfC criteria for implementation independence.	All	T=O	
MA-PS-17	The Outer firewall, Outer VPN Gateway, Gray Firewall, Inner Encryption Component, and Inner firewall shall use physically separate components, such that no component is used for more than one function (see Figure 1).	VI, TI	T=O	

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-PS-18	The Outer VPN Gateway and the Inner Encryption Endpoints shall not use the same Operating System (OS). Differences between Service Packs (SP) and version numbers for a particular vendor's OS do not provide adequate diversity.	VI, TI	T=O	
MA-PS-19	The Inner and the Outer CAs shall either: • come from different manufacturers, where neither manufacturer is a subsidiary of the other; or • be different products from the same manufacturer, where NSA has determined that the products meet the CSfC criteria for implementation independence.	VI, TI	O	Optional
MA-PS-20	The Gray Network Firewall and the Inner Encryption Endpoints shall either: • come from different manufacturers, where neither manufacturer is a subsidiary of the other; or • be different products from the same manufacturer, where NSA has determined that the products meet the CSfC criteria for implementation independence.	VI, TI	T=O	
MA-PS-21	The EUD's Outer VPN Component and Inner Encryption Components shall either: • come from different manufacturers, where neither manufacturer is a subsidiary of the other; or • be different products from the same manufacturer, where NSA has determined that the products meet the CSfC criteria for implementation independence.	VE, TE	T=O	

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-PS-22	The cryptographic libraries used by the Inner CA and Outer CA shall either: • come from different manufacturers, where neither manufacturer is a subsidiary of the other; or • be different libraries from the same manufacturer, where NSA has determined that the libraries meet the CSfC Program's criteria for implementation independence.	VI, TI	O	Optional
MA-PS-23	The cryptographic libraries used by the Outer VPN Component and the Inner Encryption Components shall either: • come from different manufacturers, where neither manufacturer is a subsidiary of the other; or • be different libraries from the same manufacturer, where NSA has determined that the libraries meet the CSfC criteria for implementation independence.	VE, TE	O	Optional
MA-PS-24	Each component that is selected out of the CSfC Components List shall go through a Product Supply Chain Threat Assessment to determine the appropriate mitigations for the intended application of the component per the organization's AO-approved Product Supply Chain Threat Assessment process (see CNSSD 505 SCRM for additional guidance).	All	T=O	
MA-PS-25	Components shall be configured to use the NIAP-certified evaluated configuration.	All	O	Optional

13 CONFIGURATION REQUIREMENTS

Once the products for the solution are selected, the next step is setting up the components and configuring them in a secure manner. This section consists of generic guidance for how to configure the components of the MA solution.

13.1 Overall Solution Requirements

Table 7. Overall Solution Requirements

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-SR-1	Network services provided by control plane protocols (such as DNS and NTP) shall be located on the inside network (i.e., Gray network for the Outer VPN Gateway and Red network for the Inner Encryption Endpoints).	VI, TI	T=O	
MA-SR-2	The time of day on Inner Encryption Endpoints, Inner firewall, and Red Management Services shall be synchronized to a time source located in the Enterprise/Red network.	VI, TI	T=O	
MA-SR-3	The time of day on the Outer VPN Gateway, Gray firewall, and Gray Management Services shall be synchronized to a time source located in the Gray Management network.	VI, TI	T=O	
MA-SR-4	Default accounts, passwords, community strings, and other default access control mechanisms for all components shall be changed or removed.	All	T=O	
MA-SR-5	All components shall be properly configured in accordance with local policy and applicable U.S. Government guidance. In the event of conflict between the requirements in this CP and local policy, this CP takes precedence.	All	T=O	
MA-SR-6	Solution Components shall receive virus signature updates as required by the local agency policy and the AO.	All	T=O	
MA-SR-7	The only approved physical paths leaving the Red network shall be through a MA solution in accordance with this CP or via an AO-approved solution for protecting data in transit.[2]	All	T=O	

[2] In some cases, the customer will need to communicate with other sites that have NSA-certified Government off-the-Shelf (GOTS) product. In particular, it is acceptable for a given site to have both an egress path via an NSA-certified product and an egress path via a CSfC Solution conforming to a CP.

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-SR-8	When multiple Inner Encryption components are placed between the Gray firewall and Inner firewall, they shall be placed in parallel.	VI, TI	T=O	
MA-SR-9	Inner Encryption components shall not perform switching or routing for other Encryption Components.	VI, TI	T=O	

13.2 CONFIGURATION REQUIREMENTS FOR ALL VPN COMPONENTS

Table 8. Approved Suite B Algorithms (IPSec)

Security Service	Algorithm Suite 2	Specifications
Overall Level of Security	192 bits	
Confidentiality (Encryption)	AES-256	FIPS PUB 197 IETF RFC 6239 IETF RFC 6379 IETF RFC 6380 IETF RFC 6460
Authentication (Digital Signature) (Threshold)	RSA 2048	FIPS PUB 186-4
Authentication (Digital Signature) (Objective)	RSA 3072 or ECDSA over the curve P-384 with SHA-384	FIPS PUB 186-4 FIPS PUB 186-4 IETF RFC 6239 IETF RFC 6380 IETF RFC 6460
Key Exchange/ Establishment	ECDH over the curve P-384 (DH Group 20)	NIST SP 800-56A IETF RFC 6239 IETF RFC 6379 IETF RFC 6380 IETF RFC 6460 NIST SP 800-56A
Integrity (Hashing)	SHA-384	FIPS PUB 180-4 IETF RFC 6239 IETF RFC 6379 IETF RFC 6380 IETF RFC 6460
Can protect	Up to Top Secret	

Table 9. Approved Algorithms (TLS)

	TLS Cipher Suites	Specifications
Overall Level of Confidentiality	192 bits	FIPS PUB 180-4 FIPS PUB 186-3 FIPS PUB 197 FIPS 800-56A IETF RFC 6460 IETF RFC 5246 IETF RFC 4492
TLS Cipher Suite (Threshold)	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	
TLS Cipher Suite (Objective)	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	
Authentication (Digital Signature) (Threshold)	RSA 2048	
Authentication (Digital Signature) (Objective)	RSA 3072 or ECDSA over the curve P-384 with SHA-384	
Key Exchange	ECDHE over the curve P-384 (DH Group 20)	
Can protect	Up to Top Secret	

Table 10. Approved Algorithms (Secure Real-Time Protocol)

Security Service	Algorithm Suite 1	Algorithm Suite 2	Specifications
Overall Level of Security	128 bits	192 bits	IETF RFC 3711 IETF RFC 6188
Confidentiality (Encryption)	AES-128 in Counter Mode (CM)	AES-256 in Counter Mode (CM)	IETF RFC 3711 IETF RFC 2675
Integrity	HMAC-SHA1	HMAC-SHA1	IETF RFC 3711 IETF RFC 2104
Key Exchange (using SIP Over TLS)	TLS-SDES or DTLS	TLS-SDES or DTLS	IETF RFC 4568 IETF RFC 6347
Can protect	Up to Secret	Up to Top Secret	

13.3 CONFIGURATION REQUIREMENTS FOR INNER AND OUTER VPN COMPONENTS

Table 11 Configuration Requirements for Inner and Outer VPN Components

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-CR-1	The proposals offered by the Outer and Inner VPN Components in the course of establishing the IKE Security Association (SA) and the ESP SA for Inner and Outer Tunnels shall be configured to only offer algorithm suite(s) containing the Suite B algorithms listed in Table 8.	All	T=O	
MA-CR-2	Default, self-signed, or proprietary device certificates, which are frequently preinstalled by the vendor, for any Outer and Inner VPN Component, shall not be used for establishing SAs.	All	T	MA-CR-3
MA-CR-3	Default, self-signed, or proprietary device certificates, which are frequently preinstalled by the vendor, for any Outer and Inner VPN Component, shall be removed.	All	O	MA-CR-2
MA-CR-4	Unique device certificates shall be loaded onto the Outer and Inner VPN Gateway along with the corresponding Trust Anchor (signing) certificates.	VI, TI	T=O	
MA-CR-5	A device certificate shall be used for each Outer and Inner VPN Component authentication during IKE.	All	T=O	
MA-CR-6	Authentication performed by Outer and Inner VPN Gateways shall include a check that device certificates are authorized. This check may use a CRL, OCSP, or a whitelist.	VI, TI	T=O	
MA-CR-7	Outer and Inner VPN Component authentication with device certificates shall include a check that certificates are not expired.	All	T=O	
MA-CR-8	Withdrawn			
MA-CR-9	All IPsec connections shall use IETF standards IKE implementations (RFC 5996 or RFC 2409).	All	T=O	
MA-CR-10	All Outer and Inner VPN Components shall use Cipher Block Chaining for IKE encryption.	All	T=O	
MA-CR-11	All Outer and Inner VPN Components shall use Cipher Block Chaining for ESP encryption with an HMAC for integrity.	All	T	MA-CR-12

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-CR-12	All Outer and Inner VPN Components shall use Galois Counter Mode for ESP encryption.	All	O	MA-CR-11
MA-CR-13	All Outer and Inner VPN Components shall set the IKE SA lifetime to at most 24 hours.	All	T=O	
MA-CR-14	All Outer and Inner VPN Components shall set the ESP SA lifetime to at most 8 hours.	All	T=O	
MA-CR-15	All VPN Components shall re-authenticate the identity of the VPN Component at the other end of the established tunnel before rekeying the IKE SA.	All	T=O	

13.4 Inner VPN Components

Table 12. Inner VPN Components Requirements

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-IR-1	The Inner VPN Component shall use Tunnel mode IPsec or Transport mode IPsec using an associated IP tunneling protocol (e.g. Transport Mode IPsec with GRE).	VI	T=O	
MA-IR-2	The packet size for packets leaving the external interface of the Inner VPN Component shall be configured to reduce packet fragmentation and impacting performance. This requires proper configuration of the Maximum Transmission Unit (MTU) (for IPv4) or Path MTU (PMTU) (for IPv6) and should consider Black network and Outer VPN component MTU/PMTU values to achieve this.	VI	O	Optional
MA-IR-3	The Inner VPN Gateway shall not allow any packets received on an interface connected to a Red network to bypass encryption and be forwarded out through an interface connected to a Gray network.	V	T=O	

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-IR-4	The Inner VPN Client of EUDs shall encrypt all traffic, with the exception of traffic necessary for the EUD to connect to the physical network (e.g. DHCP) and locate the Inner VPN Gateway (i.e. DNS lookup of the VPN Component's IP address), in accordance with this CP.	VE	T=O	
MA-IR-5	The Inner VPN Component shall not allow any packets received on an interface connected to a Gray network to bypass decryption and be forwarded out through an interface connected to a Red network.	V	T=O	

13.5 Outer VPN Components

Table 13. Outer VPN Components Requirements

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-OR-1	Outer VPN Components shall use Tunnel mode IPsec.	All	T=O	
MA-OR-2	Outer VPN Components shall not permit split-tunneling.	All	T=O	
MA-OR-3	The Outer VPN Component shall not allow any packets received on an interface connected to a Gray network to bypass encryption and be forwarded out through an interface connected to a Black network.	All	T=O	
MA-OR-4	All traffic received by the Outer VPN Component on an interface connected to a Gray network, with the exception of Control Plane traffic not prohibited in the CP, shall have already been encrypted once.	All	T=O	
MA-OR-5	The Outer VPN Client of EUDs shall encrypt all traffic, with the exception of traffic necessary for the EUD to connect to the physical network (e.g. DHCP) in accordance with this CP (see Section 4.1.4).	VE, TE	T=O	
MA-OR-6	If one or more virtual machines are used to separate Outer and Inner VPN Clients on an EUD, then the Outer VPN Client shall not run on the host operating system.	VE, TE	T=O	

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-OR-7	Outer VPN Component shall not allow any packets received on an interface connected to a Black network to bypass decryption.	All	T=O	
MA-OR-8	Withdrawn			
MA-OR-9	Outer VPN Gateways shall not perform routing.	VI, TI	T=O	

13.6 TLS-Protected Server & SRTP Endpoint Requirements

Table 14. TLS-Protected Server & SRTP Endpoint Requirements

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-TE-1	TLS Components shall utilize TLS 1.2 or later.	T	T=O	
MA-TE-2	TLS Solution Infrastructure components shall terminate the Inner layer of encryption originating from TLS EUDs.	TI	T=O	
MA-TE-3	TLS Solution Infrastructure components shall use X.509 device certificates for mutual authentication with TLS EUDs.	TI	T=O	
MA-TE-4	Default, self-signed, or proprietary certificates, which are frequently preinstalled by the vendor, for the TLS Component shall be disabled.	T	T	MA-TE-5
MA-TE-5	Default, self-signed, or proprietary certificates, which are frequently preinstalled by the vendor, for the TLS Component shall be removed.	T	O	MA-TE-4
MA-TE-6	Unique device certificates shall be loaded onto TLS Components along with the corresponding Trust Anchor (signing) certificates.	T	T=O	
MA-TE-7	TLS Components shall only use ciphers suites selected from the “TLS Cipher Suite (Threshold)” row of Table 9.	T	T	MA-TE-8
MA-TE-8	TLS Components shall only use cipher suites selected from the “TLS Cipher Suite (Objective)” row of Table 9.	T	O	MA-TE-7

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-TE-9	SRTP Components shall only use algorithms selected from Table 10 that are approved to protect the highest classification level of the Red network data.	T	T=O	

13.7 RETRANSMISSION DEVICE REQUIREMENTS

Table 15. Requirements for Retransmission Device

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-RD-1	An EUD shall only connect to Retransmission Devices (RDs) authorized by a Government AO.	VE, TE	T=O	
MA-RD-2	An RD shall provide EUDs with connectivity to the Mobile Access Solution infrastructure via any Black Network using Wi-Fi or an Ethernet cable.	VE, TE	T=O	
MA-RD-3	If the RD is configured to be a Wi-Fi access point, the Wi-Fi network shall implement WPA2 AES-CCMP PSK or WPA2-Enterprise with a TLS-based EAP method.	VE, TE	T=O	
MA-RD-4	A RD shall not be utilized to protect Gray data between an Outer VPN Gateway and EUD.	VE, TE	T=O	
MA-RD-5	If the RD is configured to be a Wi-Fi access point using PSK, then the PSK shall use a length of at least 32 hexadecimal characters (or its equivalent).	VE, TE	T	MA-EU-26
MA-RD-6	RD shall only permit connections to devices on a Media Access Control (MAC) white list.	VE, TE	O	Optional
MA-RD-7	If the RD is configured as a Wi-Fi access point, then the PSK shall not be displayed on the RD.	VE, TE	T=O	
MA-RD-8	If the RD is configured as a Wi-Fi access point, then the Service Set Identification (SSID) shall not be displayed on the RD.	VE, TE	T=O	
MA-RD-9	If the RD is configured as a Wi-Fi access point, then the MAC address of connected devices shall not be displayed on the RD.	VE, TE	T=O	

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-RD-10	The Administrator password shall not be displayed on the RD.	VE, TE	T=O	
MA-RD-11	The RD shall display the number of currently connected devices.	VE, TE	O	Optional
MA-RD-12	If the RD is configured to be a Wi-Fi access point, then Wi-Fi Protected Setup (WPS) shall be disabled.	VE, TE	T=O	
MA-RD-13	The RD shall be administered using HTTPS.	VE, TE	T=O	
MA-RD-14	The RD shall require authentication with Administrator credentials to make changes to RD settings.	VE, TE	T=O	
MA-RD-15	The RD default Administrator credentials shall be changed during provisioning.	VE, TE	T=O	
MA-RD-16	The RD shall be configured to limit the number of connected devices to the maximum required for the mission.	VE, TE	T=O	
MA-RD-17	If the RD is configured as a Wi-Fi access point, then traffic of multiple EUDs sharing the RD shall be separated (commonly referred to as Wi-Fi Privacy Separation or AP Isolation).	VE, TE	T=O	
MA-RD-18	If the RD is configured as a Wi-Fi access point, then the RD shall disable broadcasting of the SSID.	VE, TE	O	Optional
MA-RD-19	The RD shall only permit charging on USB ports and interfaces.	VE, TE	O	Optional
MA-RD-20	The RD shall not permit connected EUDs to access files stored on the RD.	VE, TE	T=O	
MA-RD-21	The RD shall require Administrator authentication prior to downloading logs or configuration files.	VE, TE	T=O	
MA-RD-22	The RD shall only allow firmware updates signed by the RD manufacturer.	VE, TE	O	Optional
MA-RD-23	The RD shall prevent the ability to boot into recovery mode.	VE, TE	O	Optional
MA-RD-24	The RD shall require user or administrator authentication prior to updating firmware.	VE, TE	O	Optional
MA-RD-25	If the RD is configured to be a Wi-Fi access point, the PSK shall use a length of at least 64 hexadecimal characters (or its equivalent).	VE, TE	O	MA-RD-5

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-RD-26	If the RD is configured to be a Wi-Fi access point using WPA Enterprise, the certificate used for authentication shall be different from the certificates utilized to authenticate the outer and inner tunnels.	VE, TE	T=O	

13.8 End User Devices Requirements

Table 16. Requirements for End User Devices

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-EU-1	EUDs which do not implement an NSA-approved DAR solution and allow a user to store classified information on the EUD shall be treated as classified at all times. (See Section 4.2.1).	TE, VE	T=O	
MA-EU-2	EUDs which implement an NSA-approved DAR solution (i.e. Data at Rest CP) shall comply with the handling requirements specified for the DAR solution.	VE, TE	T=O	
MA-EU-3	Thin EUDs which prohibit a user from storing classified information shall be treated as unclassified, or a higher classification level as determined by the AO, when powered down.	VE, TE	T=O	
MA-EU-4	The Outer VPN Client private key store shall be separate from the private key store for the Inner VPN Client.	VE TE	T=O	
MA-EU-5	The Inner and Outer VPN Clients on the EUD shall be implemented on separate IP stacks. Implementations of IPv4 and IPv6 on the same operating system are considered to be part of the same IP stack.	VE	T=O	
MA-EU-6	If the EUD is not remotely administered, then it shall only be updated and rekeyed through re-provisioning.	VE, TE	T=O	
MA-EU-7	The EUD shall not allow split-tunneling.	VE, TE	T=O	
MA-EU-8	Rekeying of an EUD's certificates and associated private keys shall be done through re-provisioning prior to expiration of keys.	VE, TE	T	MA-EU-9

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-EU-9	Rekeying of an EUD's certificates and associated private keys shall be done over the MA solution network prior to expiration of keys.	VE, TE	O	MA-EU-8
MA-EU-10	An EUD shall be deauthorized from the network and submitted for Forensic Analysis if suspected of being compromised.	VE, TE	T=O	
MA-EU-11	An EUD should be destroyed only if it has been determined to be compromised through Forensic Analysis.	VE, TE	T=O	
MA-EU-12	Users of EUDs shall successfully authenticate themselves to the services they access on the Red network using an AO-approved method.	VE, TE	T=O	
MA-EU-13	Red network services shall not transmit any classified data to EUDs until user authentication succeeds.	VE, TE	T=O	
MA-EU-14	Withdrawn			
MA-EU-15	All EUD Users shall sign an organization-defined user agreement before being authorized to use an EUD.	VE, TE	T=O	
MA-EU-16	All EUD Users shall receive an organization-developed training course for operating an EUD prior to use.	VE, TE	T=O	
MA-EU-17	At a minimum, the organization-defined user agreement shall include each of the following: • Consent to monitoring • Operations Security (OPSEC) guidance • Required physical protections to employ when operating and storing the EUD • Restrictions for when, where, and under what conditions the EUD may be used • Responsibility for reporting security incidents • Verification of IA Training • Verification of appropriate clearance • Justification for Access • Requester information and organization • Account Expiration Date • User Responsibilities	VE, TE	T=O	

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-EU-18	EUDs shall be dedicated for use solely in the Mobile Access solution, and not used to access any resources on networks other than the Red network it communicates with through the two layers of encryption.	VE, TE	T=O	
MA-EU-19	EUDs shall be remotely administered.	VE, TE	O	Optional
MA-EU-20	The EUD shall disable all transmitted Global Positioning System (GPS) and location services except Enhanced 9-1-1 (E911) or those authorized by the AO.	VE, TE	T=O	
MA-EU-21	The EUD shall disable Firmware-Over-the-Air (FOTA) updates from the cellular carrier.	VE, TE	T=O	
MA-EU-22	The EUD shall disable all wireless interfaces (e.g. Bluetooth, NFC, Cellular, 802.11) that do not pass through the VPN client.	VE, TE	T=O	
MA-EU-23	The EUD shall disable processing of incoming cellular services including voice messaging services that do not pass through the VPN client.	VE, TE	O	Optional
MA-EU-24	All EUDs shall have their certificates revoked and resident image removed prior to disposal.	VE, TE	T=O	
MA-EU-25	Passwords for user to device (EUD selected from Mobile Platform section of CSfC Components List) authentication shall be a minimum of 4 alpha-numeric case sensitive characters.	VE, TE	T=O	
MA-EU-26	Withdrawn			
MA-EU-27	For a VPN EUD that has a VPN Gateway physically attached to it, the VPN Gateway shall be the Outer layer of encryption and the VPN client on the EUD will be the Inner Layer of encryption.	VE	T=O	
MA-EU-28	Withdrawn			
MA-EU-29	If the EUD is using a physically attached VPN Gateway as the Outer layer of encryption, the communication between the EUD and the VPN Gateway shall be through a wired connection (i.e. Ethernet) or Wi-Fi using WPA2.	VE, TE	T=O	
MA-EU-30	Withdrawn			

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-EU-31	If a TLS EUD is using a standalone VPN Gateway to connect over the black transport network, the VPN Gateway shall be used to establish the Outer Layer of encryption.	TE	T=O	
MA-EU-32	If an NSA-Approved DAR Solution is not implemented on EUDs, the native platform DAR protection shall be enabled.	VE, TE	T=O	
MA-EU-33	EUDs shall use a unique X.509 v3 device certificate, signed by the Outer CA, for mutual authentication with Outer VPN Gateways.	VE, TE	T=O	
MA-EU-34	TLS EUDs shall either use a unique X.509 v3 device certificate (signed by the Inner CA) or a unique X.509 v3 user certificate (signed by an authorized enterprise services CA) for mutual authentication with TLS-Protected Servers.	TE	T =O	
MA-EU-35	VPN EUDs shall use a unique X.509 v3 device certificate, signed by the Inner CA, for mutual authentication with Inner VPN Gateways.	VE	T=O	
MA-EU-36	EUDs shall use an Access Point Name (APN) provided by a Domestic Cellular Carrier Private Network when utilizing Domestic Cellular Service as a Black Transport Network.	VE, TE	O	Optional
MA-EU-37	EUDs shall be configured for all IP traffic, with the exception of IKE, network address configuration, time synchronization, and name resolution traffic required to establish the IPsec tunnel, to flow through the IPsec VPN Client.	VE, TE	T	MA-EU-38
MA-EU-38	EUDs shall be configured for all IP traffic, with the exception of IKE, to flow through the IPsec VPN Client.	VE, TE	O	MA-EU-37
MA-EU-39	The EUD maximum password lifetime shall be less than 181 days.	VE, TE	T=O	
MA-EU-40	The EUD screen shall lock after three minutes or less of inactivity.	VE, TE	T=O	
MA-EU-41	The EUD shall perform a wipe of all protected data after 10 or less authentication failures.	VE, TE	T=O	
MA-EU-42	VPN Protection shall be enabled across the EUD.	VE, TE	T=O	
MA-EU-43	A security policy shall be configured on the EUD specific to each permitted Retransmission Device and/or Government Private Wireless network.	VE, TE	T=O	

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-EU-44	During provisioning, all unnecessary keys shall be destroyed from the EUD secure key storage.	VE, TE	T=O	
MA-EU-45	During provisioning, all unnecessary X.509 certificates shall be removed from the EUD Trust Anchor Database.	VE, TE	T=O	
MA-EU-46	All display notifications shall be disabled while in a locked state.	VE, TE	O	Optional
MA-EU-47	USB mass storage mode shall be disabled on the EUDs.	VE, TE	O	Optional
MA-EU-48	USB data transfer shall be disabled on the EUDs.	VE, TE	O	Optional
MA-EU-49	Prior to updating the Application Processor system software, the system software digital signature shall be verified.	VE, TE	T=O	
MA-EU-50	Prior to installing new applications, the application digital signature shall be verified.	VE, TE	T=O	

13.9 Port Filtering Requirements for Solution Components

Table 17. Port Filtering Requirements for Solution Components

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-PF-1	All Components within the Solution shall have all network interfaces restricted to the smallest address ranges, ports, and protocols possible.	All	T=O	
MA-PF-2	All Components within the Solution shall have all unused network interfaces disabled.	All	T=O	
MA-PF-3	CDPs shall only allow inbound HTTP traffic.	C	T=O	
MA-PF-4	For the Outer VPN Gateway interface connected to a Black network, traffic filtering rules shall be applied to both inbound and outbound traffic, such that only IKE, ESP, and control plane protocols (as defined in this CP) approved by organization-defined policy are allowed.	All	T=O	

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-PF-5	For the Inner VPN Gateway interface connected to a Gray network, traffic filtering rules shall be applied to both inbound and outbound traffic, such that only IKE, ESP, and management and control plane protocols (as defined in this CP) approved by organization-defined policy are allowed.	V	T=O	
MA-PF-6	The Inner firewall shall implement an ACL which only permits ingress/egress traffic to Inner Encryption Endpoints.	All	T=O	
MA-PF-7	Any service or feature that allows an Outer VPN Gateway or an EUD to contact a third party server (such as one maintained by the manufacturer) shall be blocked.	All	T	MA-PF-8
MA-PF-8	Any service or feature that allows an Outer VPN Gateway or an EUD to contact a third party server (such as one maintained by the manufacturer) shall be disabled.	All	O	MA-PF-7
MA-PF-9	Multicast messages received on external interfaces of Outer VPN Gateway shall be dropped.	All	T=O	
MA-PF-10	For solutions using IPv4, the Outer VPN Gateway shall drop all packets that use IP options.	All	O	Optional
MA-PF-11	For solutions using IPv4, the Outer VPN Gateway shall only accept packets with Transmission Control Protocol (TCP), User Data Protocol (UDP), Encapsulating Security Payload (ESP), or ICMP in the IPv4 Protocol field and drop all other packets.	All	T=O	
MA-PF-12	For solutions using IPv6, the Outer VPN Gateway shall only accept packets with ESP, TCP, UDP, or ICMPv6 in the IPv6 Next Header field and drop all other packets.	All	T=O	
MA-PF-13	For all Outer firewall interfaces, traffic filtering rules shall be applied to both inbound and outbound traffic, such that only IKE, ESP, and control plane protocols (as defined in this CP) approved by organization-defined policy are allowed.	VI, TI	T=O	

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-PF-14	EUDs consisting of a single computing platform shall prohibit ingress and egress of Certificate Revocation traffic (e.g. OCSP queries, HTTP GET to CDPs) on the Black interface.	VE, TE	T=O	
MA-PF-15	EUDs consisting of a single computing platform shall prohibit ingress and egress of Name Resolution traffic (e.g. DNS query/response) on the Black Interface.	VE, TE	O	Optional
MA-PF-16	EUDs consisting of a single computing platform shall prohibit ingress and egress of Network Time Protocol (NTP) traffic on the Black Interface.	VE, TE	O	Optional

13.10 Configuration Change Detection Requirements

Table 18. Configuration Change Detection Requirements

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-CM-1	A baseline configuration for all components shall be maintained by the Security Administrator and be available to the Auditor.	All	T=O	
MA-CM-2	An automated process shall ensure that configuration changes are logged.	All	T=O	
MA-CM-3	All Solution components shall be configured with a monitoring service that detects all changes to configuration.	All	O	Optional

13.11 Device Management Requirements

Only authorized Security Administrators will be allowed to administer the Components. The MA solution will be used as transport for the Secure Shell (SSH)v2, IPsec, or TLS data from the Administration Workstation to the Component.

Table 19. Requirements for Device Management

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-DM-1	Administration Workstations shall be dedicated for the purposes given in the CP and shall be physically separated from workstations used to manage non-CSfC solutions.	VI, TI	T=O	
MA-DM-2	The Inner Encryption Endpoints shall be managed from the Enterprise/Red network and the Outer VPN Gateway and Gray firewall shall be managed from the Gray network.	VI, TI	T=O	
MA-DM-3	A separate LAN or VLAN on the Enterprise/Red network shall be used exclusively for all management of Inner Encryption Endpoints and solution components within the Red network.	VI, TI	T=O	
MA-DM-4	A separate LAN or VLAN on the Gray network shall be used exclusively for all management of the Outer VPN Gateway, Gray firewall, and solution components within the Gray network.	VI, TI	T=O	
MA-DM-5	The Gray Management network shall not be directly connected to Non-secure Internet Protocol Router Network (NIPRNet) or any other Unclassified network not dedicated to the administration of CSfC solutions.	VI, TI	T=O	
MA-DM-6	All administration of solution components shall be performed from an Administration Workstation • remotely using one of SSHv2, IPsec, or TLS 1.2 or later version; or • by managing the solution components locally.	VI, TI	T=O	
MA-DM-7	Security Administrators shall authenticate to solution components before performing administrative functions.	All	T	MA-DM-8
MA-DM-8	Security Administrators shall authenticate to solution components with Suite B-compliant certificates before performing administrative functions remotely.	All	O	MA-DM-7
MA-DM-9	Security Administrators shall establish a security policy for EUDs per the implementing organization's local policy.	VE, TE	T=O	

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-DM-10	EUDs shall generate logs and send to a central SIEM in the Red network.	VE, TE	O	Optional
MA-DM-11	Security Administrators shall initiate certificate signing requests for solution components as part of their initial keying within the solution.	All	T=O	
MA-DM-12	Devices shall use Enrollment over Secure Transport (EST) as detailed in IETF RFC 7030 for certificate management.	All	O	Optional
MA-DM-13	The same Administration Workstation shall not be used to manage Inner Encryption Components and the Outer VPN Gateway.	VI, TI	T=O	
MA-DM-14	The Outer VPN Gateway and solution components within the Gray network shall forward log entries to a SIEM on the Gray Management network (or SIEM in the Enterprise/Red Network if using an AO approved one-way tap) within 10 minutes.	VI, TI	T=O	
MA-DM-15	Inner Encryption Components and solution components within the Red network shall forward log entries to a SIEM on the Red Management network within 10 minutes.	VI, TI	O	Optional
MA-DM-16	All logs forwarded to a SIEM on the Gray Management network shall be encrypted using SSHv2, IPsec, or TLS 1.1 or later.	All	O	Optional
MA-DM-17	All logs forwarded to a SIEM on a Red Management network shall be encrypted using SSHv2, IPsec, or TLS 1.1 or later.	All	O	Optional
MA-DM-18	When managing Solution components over the Black network, the management traffic shall be encrypted with Suite B algorithms IAW Table 8 and Table 9.	All	T=O	

13.12 CONTINUOUS MONITORING REQUIREMENTS

Table 20. Continuous Monitoring Requirements

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-MR-1	Traffic from the Black, Gray, or Red networks shall be monitored from an Intrusion Detection System (IDS).	VI, TI	T	MA-MR-2

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-MR-2	Traffic from the Black, Gray, or Red networks shall be monitored from an Intrusion Prevention System (IPS).	VI, TI	O	MA-MR-1
MA-MR-3	An IDS shall be deployed between the Outer firewall and Outer VPN Gateway (M1), or between the Outer VPN Gateway and the Gray firewall (M2), or on the internal side of the Inner firewall (M3).	VI, TI	T	MA-MR-4 MA-MR-5 MA-MR-6
MA-MR-4	An IDS shall be deployed between the Outer firewall and Outer VPN Gateway (M1), and between the Outer VPN Gateway and the Gray firewall (M2), and on the internal side of the Inner firewall (M3).	VI, TI	O	MA-MR-3 MA-MR-5 MA-MR-6
MA-MR-5	An IPS shall be deployed between the Outer firewall and Outer VPN Gateway (M1), or between the Outer VPN Gateway and the Gray firewall (M2), or on the internal side of the Inner firewall (M3).	VI, TI	O	MA-MR-3 MA-MR-4 MA-MR-6
MA-MR-6	An IPS shall be deployed between the Outer firewall and Outer VPN Gateway (M1), and between the Outer VPN Gateway and the Gray firewall (M2), and on the internal side of the Inner firewall.	VI, TI	O	MA-MR-3 MA-MR-4 MA-MR-5
MA-MR-7	Each IDS in the solution shall be configured to send alerts to the Security Administrator.	VI, TI	T	MA-MR-8
MA-MR-8	Each IPS in the solution shall be configured to block malicious traffic flows and alert the Security Administrator.	VI, TI	O	MA-MR-7
MA-MR-9	Each IDS in the solution shall be configured with rules that generate alerts upon detection of any unauthorized destination IP addresses.	VI, TI	T	MA-MR-10
MA-MR-10	Each IPS in the solution shall be configured with rules that block and generate alerts upon detection of any unauthorized destination IP addresses.	VI, TI	O	MA-MR-9
MA-MR-11	Each IDS in the solution shall be configured with rules that generate alerts upon detection of any unauthorized source IP addresses.	VI, TI	T	MA-MR-12
MA-MR-12	Each IPS in the solution shall be configured with rules that block and generate alerts upon detection of any unauthorized source IP addresses.	VI, TI	O	MA-MR-11

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-MR-13	A SIEM component shall be placed within the Gray network unless devices are configured to push events to an Enterprise/Red network SIEM through an AO-approved one-way tap.	VI, TI	T=O	
MA-MR-14	The SIEM shall be configured to send alerts to the Auditor when anomalous behavior is detected (i.e. blocked packets from the Outer VPN Gateway or Gray firewall).	VI, TI	T=O	
MA-MR-15	The Gray SIEM shall collect logs from the Outer VPN Gateway, Gray firewall, and any components located within the Gray Management Services.	VI, TI	T=O	
MA-MR-16	Logs sent to the Gray SIEM shall be encrypted with TLS, SSHv2, or IPsec.	VI, TI	T=O	
MA-MR-17	One-way taps deployed as part of the solution shall be approved for use by the AO.	VI, TI	T=O	
MA-MR-18	One-way taps deployed as part of the solution shall only allow monitoring data to flow from Monitoring Point 2 (M2) and/or Monitoring Point 1 (M1) to an enclave at the Red level that is isolated from the Red/Enterprise Network.	VI, TI	T=O	

13.13 AUDITING REQUIREMENTS

Table 21. Auditing Requirements

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-AU-1	VPN Gateways shall log establishment of a VPN tunnel.	T, V	T=O	
MA-AU-2	TLS-Protected Servers shall log establishment of a TLS connection.	TI	T=O	
MA-AU-3	VPN Gateways shall log termination of a VPN tunnel.	T, V	T=O	
MA-AU-4	TLS-Protected Servers shall log termination of a TLS connection.	TI	T=O	
MA-AU-5	VPN Clients shall log establishment of a VPN tunnel.	VE, TE	O	Optional
MA-AU-6	TLS Clients shall log establishment of a TLS Tunnel	TE	O	Optional
MA-AU-7	VPN Clients shall log termination of a VPN tunnel.	VE, TE	O	Optional

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-AU-8	TLS Client shall log termination of a TLS Tunnel.	TE	O	Optional
MA-AU-9	Solution components shall log all actions performed on the audit log (off-loading, deletion, etc.).	VI, TI	T=O	
MA-AU-10	Solution components shall log all actions involving identification and authentication.	VI, TI	T=O	
MA-AU-11	Solution components shall log attempts to perform an unauthorized action (read, write, execute, delete, etc.) on an object.	TI,VI	T=O	
MA-AU-12	Solution components shall log all actions performed by a user with super-user or administrator privileges.	VI, TI	T=O	
MA-AU-13	Solution components shall log escalation of user privileges.	VI, TI	T=O	
MA-AU-14	Solution components shall log generation, loading, and revocation of certificates.	All	T=O	
MA-AU-15	Solution components shall log changes to time.	VI, TI	T=O	
MA-AU-16	Each log entry shall record the date and time of the event.	All	T=O	
MA-AU-17	Each log entry shall include the identifier of the event.	All	T=O	
MA-AU-18	Each log entry shall record the type of event.	All	T=O	
MA-AU-19	Each log entry shall record the success or failure of the event to include failure code, when available.	All	T=O	
MA-AU-20	Each log entry shall record the subject identity.	All	T=O	
MA-AU-21	Each log entry shall record the source address for network-based events.	All	T=O	
MA-AU-22	Each log entry shall record the user and, for role-based events, role identity, where applicable.	All	T=O	
MA-AU-23	Auditors shall detect when two or more simultaneous VPN connections from different IP addresses are established using the same EUD device certificate.	V	O	Optional
MA-AU-24	Auditors shall detect when two or more simultaneous TLS connections from different IP addresses are established using the same EUD device certificate.	T	O	Optional

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-AU-25	Upon notification of two or more simultaneous VPN connections from different IP addresses using the same EUD device certificate, the Certificate Authority Administrator shall revoke the device certificate and provide an updated CRL to the Security Administrator.	V	O	Optional
MA-AU-26	Upon notification of two or more simultaneous TLS connections from different IP addresses using the same EUD device certificate, the Certificate Authority Administrator shall revoke the device certificate and provide an updated CRL to the Security Administrator.	T	O	Optional
MA-AU-27	The Security Administrator shall immediately drop the session upon notification of two or more simultaneous VPN connections from different IP addresses using the same EUD device certificate.	V	O	Optional
MA-AU-28	The Security Administrator shall immediately drop the session upon notification of two or more simultaneous TLS connections from different IP addresses using the same EUD device certificate.	T	O	Optional
MA-AU-29	VPN Gateways shall log the failure to download a CRL from a CDP.	VI	T=O	
MA-AU-30	TLS-Protected Servers shall log the failure to download a CRL from a CDP.	TI	T=O	
MA-AU-31	VPN Gateways shall log if the version of the CRL downloaded from a CDP is older than the current cached CRL.	VI	T=O	
MA-AU-32	TLS-Protected Servers shall log if the version of the CRL downloaded from a CDP is older than the current cached CRL.	TI	T=O	
MA-AU-33	VPN Gateways shall log if signature validation of the CRL downloaded from a CDP fails.	VI	T=O	
MA-AU-34	TLS-Protected Servers shall log if signature validation of the CRL downloaded from a CDP fails.	TI	T=O	
MA-AU-35	Auditors shall compare and analyze collected network flow data against the established baseline on at least a weekly basis.	VI, TI	O	Optional

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-AU-36	Locally-run CAs shall comply with the audit and archival requirements defined in IETF RFC 3647 Sections 4.5.4 and 4.5.5, respectively.	VI, TI	T=O	
MA-AU-37	Locally-run CAs shall comply with periodic audit and assessment requirements defined in IETF RFC 3647 Section 4.8.	VI, TI	T=O	
MA-AU-38	Audits and assessments for Outer and Inner CAs shall be performed by personnel who are knowledgeable in the CAs' operations, as well as the CAs' CP and CPS requirements and processes, respectively.	VI, TI	T=O	

13.14 Key Management Requirements

13.14.1 General Requirements

Table 22. PKI General Requirements

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-KM-1	User certificates and user private keys shall be classified to the level determined by the AO.	TE, VE	T=O	
MA-KM-2	Outer CAs shall provide services through either the Gray or Red network.	VI, TI	T = O	
MA-KM-3	Inner CAs shall provide services through the Enterprise/Red network.	VI, TI	T=O	
MA-KM-4	Locally run Inner Tunnel CAs shall be physically separate from locally-run Outer Tunnel CAs.	VI, TI	T=O	
MA-KM-5	All certificates issued by the Outer and Inner CAs for the MA Solution shall be Non-Person Entity (NPE) certificates, except in the one case when a TLS EUD requires a user certificate for the inner TLS tunnel.	VI, TI	T=O	
MA-KM-6	All certificates issued by the Outer and Inner CAs for the MA Solution shall be used for authentication only.	VI, TI	T=O	
MA-KM-7	Authentication certificates issued by the Outer and Inner CAs for the MA Solution shall be X.509 v3 certificates as defined in ITU-T Recommendation X.509.	VI, TI	T=O	

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-KM-8	Authentication certificate profiles for the Outer and Inner CAs for the MA Solution shall comply with IETF RFC 5280.	VI, TI	T=O	
MA-KM-9	All device certificates issued by the Outer and Inner CAs, and their corresponding private keys, shall be treated as CUI (or higher as determined by the AO).	All	T=O	
MA-KM-10	The key sizes and algorithms for CA certificates and authentication certificates issued to Outer VPN Components, Inner Encryption Components, and Administrative Device Components shall be as specified in CNSSP 15 (See Table 8-.	All	T=O	
MA-KM-11	Outer and Inner CAs shall not have access to private keys used in the MA Solution Components.	All	T=O	
MA-KM-12	Private keys associated with on-line, locally run Outer and Inner CAs shall be protected using Hardware Security Modules (HSMs) validated to at least FIPS 140-2 Level 2. "On-line" means the CA is always powered on and network-accessible.	VI, TI	T=O	
MA-KM-13	Outer and Inner CAs shall operate in compliance with a Certificate Policy and Certification Practices Statement that is formatted in accordance with Internet Engineering Task Force (IETF) Request for Comments (RFC) 3647.	VI, TI	T=O	

13.14.2 CERTIFICATE ISSUANCE REQUIREMENTS

Table 23. Certificate Issuance Requirements

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-KM-14	Outer VPN Components, Inner Encryption Components, and Gray and Red Management Services Components shall be initially keyed and loaded with certificates within a physical environment certified to protect the highest classification level of the MA solution network.	All	T=O	

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-KM-15	Private keys for Outer VPN Components, Inner Encryption Components and Gray and Red Management Services Components shall never be escrowed.	All	T=O	
MA-KM-16	Outer and Inner CAs shall use Public Key Cryptographic Standard (PKCS)#10 and PKCS#7 to issue authentication certificates to Outer VPN Components, Inner Encryption Components, and Gray and Red Management Services Components.	VI, TI	T	MA-KM-19
MA-KM-17	Red and Gray Management Services shall use PKCS#12 for installing certificates/keys to EUDs.	All	T	MA-KM-18
MA-KM-18	Red and Gray Management Services shall use PKCS#7 for installing certificates to EUDs.	All	O	MA-KM-17
MA-KM-19	Outer and Inner CAs shall use IETF RFC 7030 Enrollment over Secure Transport (EST) to issue authentication certificates to Outer VPN Components, Inner Encryption Components, and Gray and Red Management Services Components.	All	O	MA-KM-16
MA-KM-20	Certificate requests for Outer VPN Components, Inner Encryption Components and Gray and Red Management Services Components shall be submitted to the CA in accordance with the CA's Certificate Policy (CP) and Certification Practices Statement (CPS).	All	T=O	
MA-KM-21	Outer and Inner CAs shall issue certificates in accordance with their Certificate Policies and CPSs.	All	T=O	
MA-KM-22	Certificate Policies and CPSs for non-Enterprise, locally run CAs shall ensure the CAs issue certificates within a defined and limited name space and assert: • Unique Distinguished Names (DNs) • Appropriate key usages • A registered policy Object Identifier (OID)	All	T=O	

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-KM-23	Inner and Outer CAs shall assert at least one CRL Distribution Point (CDP) Uniform Resource Locater (URL) in certificates issued to Solution Infrastructure Outer VPN Gateways, Inner Encryption Components, and Gray and Red Management Services Components. The CDP URL specifies the location of the CAs' CRLs.	All	T=O	
MA-KM-24	The key validity period for certificates issued by non-Enterprise, locally run CAs to MA End User Devices shall not exceed 14 months.	All	T=O	
MA-KM-25	The key validity period for certificates issued by non-Enterprise, locally run CAs to MA Solution Infrastructure Components shall not exceed 36 months.	All	T=O	
MA-KM-26	Inner CAs shall only issue certificates to Inner Encryption Components and Red Network Components of MA Solutions.	All	T=O	
MA-KM-27	Outer CAs shall only issue certificates to Outer VPN Components and Gray Network Components of MA Solutions.	All	T=O	
MA-KM-28	Withdrawn			
MA-KM-29	Withdrawn			

13.14.3 CERTIFICATE RENEWAL AND REKEY REQUIREMENTS

Table 24. Certificate Renewal and Rekey Requirements

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-KM-30	Certificate renewal or rekey shall occur prior to a certificate expiring. If renewal/rekey occurs after a certificate expires, then the initial certificate issuance process is used to renew/rekey the certificate.	All	T=O	
MA-KM-31	Certificate renewal or rekey shall be performed in accordance with the CA's Certificate Policy and CPS.	All	T=O	
MA-KM-32	Inner and Outer CAs shall issue renewed/ rekeyed authentication certificates to Solution Components using PKCS#10 and PKCS#7.	All	T	MA-KM-35
MA-KM-33	Withdrawn			
MA-KM-34	Withdrawn			

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-KM-35	Inner and Outer CAs shall issue renewed/rekeyed authentication certificates to Solution Components using EST (RFC 7030).	All	O	MA-KM-32

13.14.4 CERTIFICATE REVOCATION AND CDP REQUIREMENTS

Table 25. Requirements for Certificate Revocation and CDPs

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-KM-36	Inner and Outer CAs shall revoke a certificate issued to Solution Components when the binding between the subject information and public key within the certificate issued is no longer considered valid.	VI, TI	T=O	
MA-KM-37	Inner and Outer CAs shall make certificate revocation information available in the form of CRLs signed by the CAs.	VI, TI	T=O	
MA-KM-38	CRLs shall be X.509 v2 CRLs as defined in ITU-T Recommendation X.509.	C	T=O	
MA-KM-39	CRL profiles shall comply with IETF RFC 5280.	C	T=O	
MA-KM-40	Procedures for requesting certificate revocation shall comply with the CA's Certificate Policy and Certification Practices Statement.	All	T=O	
MA-KM-41	Certificate Policies and CPSs for non-Enterprise, locally run CAs shall ensure revocation procedures address the following: • Response for a lost, stolen or compromised MA EUD • Removal of a revoked infrastructure device (i.e., VPN Gateway) from the network • Re-establishment of an MA Solution Component whose certificate was revoked • Revocation of certificates due to compromise of an MA EUD • Revocation of an authentication certificate if simultaneous use of the certificate is detected from different IP addresses	All	T=O	

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-KM-42	Inner and Outer CAs shall make CRLs available to authorized CRL Distribution Points (CDPs), so that the CRLs can be accessed by Solution Components.	C	T=O	
MA-KM-43	Enterprise CAs shall create and publish CRLs in accordance with the Enterprise CAs' Certificate Policies and CPSs.	VI, TI	T=O	
MA-KM-44	Non-enterprise, locally run CAs shall publish new CRLs at least once every 28 days.	VI, TI	T=O	
MA-KM-45	Non-enterprise, locally run CAs shall create a new CRL within one hour of a certificate being revoked.	VI, TI	T=O	
MA-KM-46	Solution Infrastructure Components shall have access to new certificate revocation information within 24 hours of the CA creating a new CRL.	VI, TI	T=O	
MA-KM-47	Non-enterprise, locally run CAs shall ensure that newly created CRLs are published at least 7 days prior to the expiration of the current CRLs.	VI, TI	T=O	
MA-KM-48	The Solution shall provide certificate revocation status information via an Online Certificate Status Protocol (OCSP) Server on the Red and Gray network that is compliant with IETF RFC 6960.	VI, TI	O	Optional
MA-KM-49	Certificate revocation status messages delivered by an OCSP server shall be digitally signed and compliant with IETF RFC 6960.	VI, TI	O	Optional

14 REQUIREMENTS FOR SOLUTION OPERATION, MAINTENANCE, AND HANDLING

14.1 REQUIREMENTS FOR THE USE AND HANDLING OF SOLUTIONS

The following requirements shall be followed regarding the use and handling of the solution.

Table 26. Requirements for the Use and Handling of Solutions

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-GD-1	All Solution Infrastructure components shall be physically protected as classified devices, classified at the level of the Enterprise/Red network.	VI, TI	T=O	
MA-GD-2	Only authorized and appropriately cleared (or escorted) administrators and security personnel shall have physical access to the solution Infrastructure components.	VI, TI	T=O	
MA-GD-3	Only authorized and appropriately cleared users, administrators, and security personnel shall have physical access to EUDs when in a classified state.	VE, TE	T=O	
MA-GD-4	All components of the solution shall be disposed of as classified devices, unless declassified using AO-approved procedures.	All	T=O	
MA-GD-5	EUDs using an NSA-approved DAR solution shall be disposed of in accordance with the disposal requirements for the DAR solution.	VE, TE	T=O	
MA-GD-6	All EUDs shall have their certificates revoked prior to disposal.	VE, TE	T=O	
MA-GD-7	Users shall periodically inspect the physical attributes of EUDs for signs of tampering or other unauthorized changes.	VE, TE	T=O	
MA-GD-8	Acquisition and procurement documentation shall not include information about how the equipment will be used, to include that it will be used to protect classified information.	All	T=O	
MA-GD-9	The solution owner shall allow, and fully cooperate with, NSA or its authorized agent to perform an IA compliance audit (including, but not limited to, inspection, testing, observation, interviewing) of the solution implementation to ensure it meets the latest version of the CP.	All	T=O	
MA-GD-10	The AO will ensure that a compliance audit shall be conducted every year against the latest version of the MA CP as part annual solution re-registration process.	All	T=O	
MA-GD-11	Results of the compliance audit shall be provided to and reviewed by the AO.	All	T=O	

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-GD-12	Customers interested in registering their solution against the MA CP shall register with NSA and receive approval prior to AO authorization to operate.	All	T=O	
MA-GD-13	The implementing organization shall complete and submit an MA CP requirements compliance matrix to their respective AO.	All	T=O	
MA-GD-14	Registration and re-registration against the MA CP shall include submission of MA CP registration forms and compliance matrix to NSA.	All	T=O	
MA-GD-15	When a new approved version of the MA CP is published by NSA, the AO shall ensure compliance against this new CP within 6 months.	All	T=O	
MA-GD-16	Solution implementation information, which was provided to NSA during solution registration, shall be updated annually (in accordance with Section 16.3) as part annual solution re-registration process.	All	T=O	
MA-GD-17	Audit log data shall be maintained for a minimum of 1 year.	All	T=O	
MA-GD-18	The amount of storage remaining for audit events shall be assessed quarterly in order to ensure that adequate memory space is available to continue recording new audit events.	All	T=O	
MA-GD-19	Audit data shall be frequently off-loaded to a backup storage medium.	All	T=O	
MA-GD-20	A set of procedures shall be developed by the implementing organization to provide guidance for identifying and reporting security incidents associated with the audit events to the proper authorities and to the data owners.	All	T=O	
MA-GD-21	The implementing organization shall develop a continuity of operations plan for auditing capability which includes a mechanism or method for determining when the audit log is reaching its maximum storage capacity.	All	T=O	

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-GD-22	The implementing organization shall develop a continuity of operations plan for auditing capability which includes a mechanism or method for off-loading audit log data for long-term storage.	All	T=O	
MA-GD-23	The implementing organization shall develop a continuity of operations plan for auditing capability which includes a mechanism or method for responding to an overflow of audit log data within a product.	All	T=O	
MA-GD-24	The implementing organization shall develop a continuity of operations plan for auditing capability which includes a mechanism or method for ensuring that the audit log can be maintained during power events.	All	T=O	
MA-GD-25	Strong passwords shall be used that comply with the requirements of the AO.	VI, TI	T=O	
MA-GD-26	Security critical patches shall be tested and subsequently applied to all components in the solution in accordance with local policy and this CP.	All	T=O	
MA-GD-27	Local policy shall dictate how the Security Administrator will install patches to solution components.	All	T=O	
MA-GD-28	Solution components shall comply with local TEMPEST policy.	All	T=O	
MA-GD-29	Software, settings, keys, and all other configuration data persistently stored on EUDs shall be handled as controlled unclassified information or higher classification.	All	T=O	
MA-GD-30	All hardware components shall be tracked through an AO-approved inventory management process that identifies each component as part of a CSfC Solution.	All	T=O	

Additional MA-GD requirements can be found in Section 15.

14.2 Requirements for Incident Reporting

Table 27 lists requirements for reporting security incidents to NSA to be followed in the event that a solution owner identifies a security incident which affects the solution. These reporting requirements are intended to augment, not replace, any incident reporting procedures already in use within the solution owner's organization. It is critical that Security Administrators, Certificate Authority

Administrators (CAAs), and Auditors are familiar with maintaining the solution in accordance with this CP. Based on familiarity with the known-good configuration of the solution, personnel responsible for the operations and maintenance of the solution will be better equipped to identify reportable incidents.

For the purposes of incident reporting, "malicious" activity includes not only events that have been attributed to activity by an adversary but also any events that are unexplained. In other words, an activity is assumed to be malicious unless it has been determined to be the result of known non-malicious activity.

Table 27 only provides requirements directly related to the incident reporting process. See Section 13.12 for requirements supporting the detection of events that may reveal that a reportable incident has occurred.

Table 27. Incident Reporting Requirements

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-RP-1	Solution owners shall report confirmed incidents meeting the criteria in MA-RP-3 through MA-RP-16 within 24 hours of detection via Joint Incident Management System (JIMS) or contacting NSA as specified in the CSfC Registration Letter issued for the solution.	All	T=O	
MA-RP-2	At a minimum, the organization shall provide the following information when reporting security incidents: • CSfC Registration Number • Point of Contact (POC) name, phone, email • Alternate POC name, phone, email • Classification level of affected solution • Name of affected Network(s) • Affected component(s) manufacturer/vendor • Affected component(s) model number • Affected component(s) version number • Date and time of incident • Description of incident • Description of remediation activities Is Technical Support from NSA requested? (Yes/No)	All	T=O	
MA-RP-3	Solution owners shall report a security failure in any of the CSfC solution components.	All	T=O	

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-RP-4	Solution owners shall report any evidence of a compromise or spillage of classified data caused by a failure of the CSfC Solution.	All	T=O	
MA-RP-5	For all Gray network interfaces, solution owners shall report any malicious inbound and outbound traffic.	All	T=O	
MA-RP-6	Solution owners shall report any evidence of an unauthorized device/user gaining access to the classified network via the solution.	All	T=O	
MA-RP-7	Solution owners shall report if a solution component sends traffic with an unauthorized destination address.	All	T=O	
MA-RP-8	Solution owners shall report any malicious configuration changes to the components.	All	T=O	
MA-RP-9	Solution owners shall report any unauthorized escalation of privileges to any of the CSfC solution components.	All	T=O	
MA-RP-10	Solution owners shall report if two or more simultaneous VPN connections from different IP addresses are established using the same EUD device certificate.	All	T=O	
MA-RP-11	Solution owners shall report any evidence of malicious physical tampering with solution components.	All	T=O	
MA-RP-12	Solution owners shall report any evidence that one or both of the layers of the solution failed to protect the data.	All	T=O	
MA-RP-13	Solution owners shall report any significant degradation of services provided by the solution.	All	T=O	
MA-RP-14	Solution owners shall report malicious discrepancies in the number of VPN connections established by Outer VPN Gateways.	All	T=O	
MA-RP-15	Solution owners shall report malicious discrepancies in the number of VPN connections established by the Inner VPN Gateway	All	T=O	
MA-RP-16	Solution owners shall report malicious discrepancies in the number of TLS connections established by the TLS-Protected Server	T	T=O	

15 ROLE-BASED PERSONNEL REQUIREMENTS

The roles required to administer and maintain the solution are defined below, along with doctrinal requirements for these roles.

Security Administrator – The Security Administrator shall be responsible for maintaining, monitoring, and controlling all security functions for the entire suite of products composing the MA solution. Security Administrator duties include but are not limited to the following:

1) Ensuring that the latest security-critical software patches and updates (such as Information Assurance Vulnerability Alerts (IAVAs)) are applied to each product.

2) Documenting and reporting security-related incidents to the appropriate authorities.

3) Coordinating and supporting product logistic support activities including integration and maintenance. Some logistic support activities may require that the Security Administrator escort uncleared personnel.

4) Employing adequate defenses of auxiliary network devices to enable proper and secure functionality of the MA solution.

5) Ensuring that the implemented MA solution remains compliant with the latest version of this CP.

6) Provisioning and maintaining EUDs in accordance with this CP for implementations that include them.

Certificate Authority Administrator (CAA) – The CAA shall be responsible for maintaining, monitoring, and controlling all security functions for the CA products. CAA duties include but are not limited to the following:

1) Administering the CA, including authentication of all components requesting certificates.

2) Maintaining and updating the CRL.

3) Provisioning and maintaining EUD certificates in accordance with this CP for implementations that include them.

Auditor – The Auditor shall be responsible for reviewing the actions performed by the Security Administrator and CAA and events recorded in the audit logs to ensure that no action or event represents a compromise to the security of the MA solution. Auditor duties include but are not limited to the following:

1) Reviewing, managing, controlling, and maintaining security audit log data.

2) Documenting and reporting security-related incidents to the appropriate authorities.

3) The Auditor will only be authorized access to Outer and Inner administrative components.

Solution Integrator – In certain cases, an external integrator may be hired to implement an MA solution based on this CP. Solution Integrator duties may include but are not limited to:

1) Acquiring the products that compose the solution.

2) Configuring the MA solution in accordance with this CP.

3) Documenting, testing, and maintaining the solution.

4) Responding to incidents affecting the solution.

End User –An End User may operate an EUD from physical locations not owned, operated, or controlled by the government. The End User shall be responsible for operating the EUD in accordance with this CP and an organization-defined user agreement. Remote User duties include, but are not limited to the following:

1) Ensuring the EUD is only operated in physical spaces which comply with the end user agreement.

2) Alerting the Security Administrator immediately upon a EUD being lost, stolen, or suspected of being tampered with.

Additional policies related to the personnel that perform these roles in an MA Solution are as follows:

Table 28. Role-Based Personnel Requirements

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-GD-31	The Security Administrator, CAAs, Auditor, EUD User, and Solution Integrators shall be cleared to the highest level of data protected by the Solution. When an Enterprise CA is used in the solution, the CAA already in place may also support this solution, provided they meet this requirement.	All	T=O	
MA-GD-32	The Security Administrator, CAA, and Auditor roles shall be performed by different people.	All	T=O	
MA-GD-33	All Security Administrators, CAAs, EUD Users, and Auditors shall meet local Information Assurance (IA) training requirements.	All	T=O	
MA-GD-34	The CAA(s) for the Inner tunnel shall be different individuals from the CAA(s) for the Outer tunnel.	All	O	Optional

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-GD-35	Upon discovering an EUD is lost or stolen, an EUD User shall immediately report the incident to their Security Administrator and Certificate Authority Administrator.	VE, TE	T=O	
MA-GD-36	Upon notification of a lost or stolen EUD, the Certificate Authority Administrators shall revoke that EUD's certificates.	VE, TE	T=O	
MA-GD-37	The Security Administrator(s) for the Inner Encryption Endpoints and supporting components on Enterprise/Red networks shall be different individuals from the Security Administrator(s) for the Outer VPN Gateway and supporting components on Gray networks.	All	T=O	
MA-GD-38	Administrators shall periodically inspect the physical attributes of infrastructure hardware for signs of tampering or other unauthorized changes.	All	O	Optional
MA-GD-39	The Auditor shall review all logs specified in this CP at least once a week.	All	T=O	
MA-GD-40	Security Administrators shall initiate the certificate revocation process prior to disposal of any solution component.	All	T=O	
MA-GD-41	Auditing of the Outer and Inner CA operations shall be performed by individuals who were not involved in the development of the CP and CPS, or integration the MA solution.	All	T=O	

16 INFORMATION TO SUPPORT AO

This section details items that likely will be necessary for the customer to obtain approval from the system AO. The customer and AO have obligations to perform the following:

- The customer, possibly with support from a System Integrator, instantiates a solution implementation that follows the NSA-approved CP.
- The customer has a testing team develop a test plan and perform testing of the MA solution, see Section 16.1.
- The customer has system certification and accreditation performed using the risk assessment information referenced in Section 16.2.

- The customer provides the results from testing and system certification and accreditation to the AO for use in making an approval decision. The AO is ultimately responsible for ensuring that all requirements from the CP have been properly implemented in accordance with the CP.
- The customer registers the solution with NSA and re-registers yearly to validate its continued use as detailed in Section 16.3.
- Customers who want to use a variant of the solution detailed in this CP will contact their NSA/IAD Client Advocate to determine ways to obtain NSA approval.
- The AO will ensure that a compliance audit shall be conducted every year against the latest version of the MA CP, and the results shall be provided to the AO.
- The AO will ensure that certificate revocation information is updated on all the Solution Components in the solution in the case of a compromise.
- The AO will ensure that any Layer 2 or Layer 3 control plane protocols that are used in the solution are necessary for the operation of the network and that local policy supports their use.
- The AO will report incidents affecting the solution in accordance with Section 14.2.

The system AO maintains configuration control of the approved solution implementation over the lifecycle of the solution. Additionally, the AO shall ensure that the solution remains properly configured with all required security updates implemented.

16.1 Solution Testing

This section provides a framework for a Test and Evaluation (T&E) plan and procedures to validate the implementation of an MA solution. This T&E will be a critical part of the approval process for the AO, providing a robust body of evidence that shows compliance with this CP.

The security features and operational capabilities associated with the use of the solution shall be tested. The following is a general high-level methodology for developing the test plan and procedures and for the execution of those procedures to validate the implementation and functionality of the MA solution. The entire solution, to include each component described in Section 5 and 6, is addressed by this test plan including the following:

1) Set up the baseline network and configure all components.
2) Document the baseline network configuration. Include product model and serial numbers, and software version numbers at a minimum.

3) Develop a test plan for the specific implementation using the test requirements from Section 17. Any additional requirements imposed by the local AO should also be tested, and the test plan shall include tests to ensure that these requirements do not interfere with the security of this solution as described in this CP.

4) Perform testing using the test plan derived in Step 3. Network testing will consist of both Black box testing and Gray box testing. A two-person testing approach should be used to administer the tests. During test execution, security and non-security related discrepancies with the solution shall be documented.

5) Compile findings, to include comments and vulnerability details as well as possible countermeasure information, into a Final Test Report to be delivered to the AO for approval of the solution.

The following testing requirement has been developed to ensure that the MA solution functions properly and meets the configuration requirements from Section 13. Testing of these requirements should be used as a minimum framework for the development of the detailed test plan and procedures.

Table 29. Test Requirements

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-TR-1	The organization implementing the CP shall perform all tests listed in Section 17.	All	T=O	

16.2 Risk Assessment

The risk assessment of the MA solution presented in this CP focuses on the types of attacks that are feasible against this solution and the mitigations that can be employed. Customers should contact their NSA/IAD Client Advocate to request this document, or visit the Secret Internet Protocol Router Network (SIPRNet) CSfC site for information. The process for obtaining the risk assessment is available on the SIPRNet CSfC website. The AO shall be provided a copy of the NSA risk assessment for their consideration in approving the use of the solution.

16.3 Registration of Solutions

All customers using CSfC solutions to protect information on National Security Systems shall register their solution with NSA prior to operational use. This registration will allow NSA to track where MA CP solutions are instantiated and to provide the AOs at those sites with appropriate information, including any significant vulnerabilities that may be discovered in components or high-level designs approved for these solutions. The CSfC solution registration process is available at http://www.nsa.gov/ia/programs/csfc_program.

Solution registrations are valid for one year from the date the solution registration is approved, at which time customers are required to re-register their solution in order to continue using it. Approved CPs will be reviewed twice a year, or as events warrant. Registered users of this CP will be notified when an updated version is published. When a new version of this CP that has been approved by the IAD Director is published, customers will have six months to bring their solutions into compliance with the new version of the CP and re-register their solution (see requirement MA-GD-15). Customers are also required to update their registrations whenever the information provided on the registration form changes.

17 TESTING REQUIREMENTS

This section contains the specific tests that allow the Security Administrator or System Integrator to ensure that they have properly configured the solution. As defined in Section 11, in order to comply with this CP, a solution must at minimum implement all Threshold requirements associated with each of the capabilities it supports, and should implement the Objective requirements associated with those capabilities where feasible. These tests may also be used to provide evidence to the AO regarding compliance of the solution with this CP. Note that the details of the procedures are the responsibility of the final developer of the solution test plan in accordance with AO-approved network procedures. The AO is ultimately responsible for ensuring that all requirements from the CP have been properly implemented.

17.1 PRODUCT SELECTION

This section contains procedures to verify that the components in this CP were selected to ensure independence in several important features.

Requirements being tested: MA-PS-1 through MA-PS-25

Procedure Description:

1) For the Inner and Outer VPN Components, perform the following:

   a) Verify that the Inner and Outer VPN Gateways are on the list of IPsec VPN Gateways on the CSfC Components List. (MA-PS-1 and MA-PS-2)

   b) Verify that the Inner and Outer VPN Clients are on the list of IPsec VPN Clients on the CSfC Components List. (MA-PS-3 and MA-PS-4)

2) For the Outer VPN Gateway and Inner Encryption Components, perform the following:

a) Verify that the Outer VPN Gateway and the Inner Encryption Endpoints either come from different independent manufacturers or that NSA has determined that sufficient implementation independence exists. (MA-PS-16)

b) Verify that the Outer VPN Gateway and Inner Encryption Components are logically separated using an NSA-approved mechanism. (MA-PS-18)

c) Verify that the Outer VPN Gateway and the Inner Encryption Endpoints are not using the same Operating System. (MA-PS-20)

d) Verify that the cryptographic libraries used by the Outer VPN Gateway and the Inner Encryption Components either come from different independent manufacturers or that NSA has determined that sufficient implementation independence exists. (MA-PS-25)

3) For each TLS-Protected Server, perform the following:

a) Verify that each TLS-Protected Server is on the CSfC Components list. (MA-PS-10)

4) For each SRTP Endpoint, perform the following:

a) Verify that each SRTP Endpoint is on the CSfC Components list. (MA-PS-12)

5) For each CA, perform the following:

a) Verify the Inner and Outer CAs came from the list of CAs on the CSfC Components List or are Enterprise CAs. (MA-PS-5)

b) Verify that the Inner and Outer CAs either come from different independent manufacturers or that NSA has determined that sufficient implementation independence exists. (MA-PS-21)

c) Verify that the cryptographic libraries used by the Inner and Outer CAs either come from different independent manufacturers or that NSA has determined that sufficient implementation independence exists. (MA-PS-24)

6) For the IPS, perform the following:

a) Verify that the IPS is from the list of IPS's on the CSfC Components Lists. (MA-PS-7)

7) For the SIP Server, perform the following:

a) Verify that the SIP Server is from the list of SIP Servers on the CSfC Components List. (MA-PS-11)

8) For the Outer, Gray, and Inner firewall, perform the following:

a) Verify that the firewalls are on the list of firewalls on the CSfC Components List. (MA-PS-13)

9) For each EUD, perform the following:

   a) Verify that the Mobile Platform EUD platform is on the list of Mobile Platforms on the CSfC Components List. (MA-PS-6)

   b) Verify that the TLS Client is chosen from the VoIP, Email, or Web Browser Applications from the CSfC Components List. (MA-PS-8)

   c) If using an SRTP Client, verify that the SRTP Client is chosen from the VoIP Applications from the CSfC Components List. (MA-PS-9)

   d) Verify that the EUD's Outer VPN Component and the Inner Encryption Components either come from different independent manufacturers or that NSA has determined that sufficient implementation independence exists. (MA-PS-23)

10) For the MDM, perform the following:

   a) Verify that the MDM is from the list of MDMs on the CSfC Components List. (MA-PS-14)

11) Verify that the Outer VPN Gateway and the Outer firewall are logically separated using an NSA-approved mechanism. (MA-PS-17)

12) Verify that the Inner Encryption Endpoints and the Gray firewall are logically separated using an NSA-approved mechanism. (MA-PS-19)

13) Verify that the Gray network firewall and the Inner Encryption Endpoints either come from different independent manufacturers or that NSA has determined that sufficient implementation independence exists. (MA-PS-22)

14) For all components used, review the mitigations in the Product Supply Chain Threat Assessment. Ensure that mitigations identified in the assessment are implemented according to the implementing organization's AO-approved Product Supply Chain Threat Assessment process. (MA-PS-26)

Expected Result:

The results of the inspection should reveal that the MA Solution components conform to the MA CP.

17.2 Physical Layout of Solution

This section contains a procedure to create an accurate record of the physical components composing the MA solution (including workstations, VPN Gateways, Inner Encryption Endpoints, CAs, and wiring). The test will also ensure that the physical implementation of the MA solution matches one of the high-level designs given in the MA CP.

Requirements being tested: MA-SR-1, MA-SR-7, MA-SR-8

Procedure Description:

1) Ensure that there are no wireless or physical connection to the solution that are not included in this CP, which may allow for traffic to leave a Red or Gray network in a manner that does not go through the MA solution (or an NSA-certified encryptor). (MA-SR-7)

2) Verify that the physical location of any network services for the Outer VPN Gateway is located on the appropriate Gray Management network. Similarly, these components for the Inner Encryption Endpoints will be located on the appropriate Red network. (MA-SR-1)

3) Verify that when using multiple Inner Encryption Components that those components are placed parallel between the Gray firewall and Inner firewall. (MA-SR-8)

Expected Result:

For Step 1, there should be no extraneous wireless or physical connections allowing data to leave Red or Gray networks besides through the MA solution (or an NSA-certified encryptor). For Step 2, Gray Management network traffic should be separate from Gray network traffic. For Step 3, Inner Encryption Components are accurately placed.

17.3 TLS-Protected Server Configurations

This section contains a procedure to ensure that the configurations for TLS-Protected Server in the MA solution follow the requirements given in this CP.

Requirements being tested: MA-TE-1 through MA-TE-9

Procedure Description:

1) For each TLS-Protected Server verify in the policy the following:

   a) Obtain the current configuration for the TLS-Protected Server.

   b) Verify that X.509 device certificates are loaded. (MA-TE-3)

   c) Verify that a unique device certificate is loaded with the corresponding CA signing certificate. (MA-TE-6)

   d) Verify the requirements MA-TE-1 through MA-TE-2, MA-TE-4, MA-TE-5, and MA-TE-7 through MA-TE-9 are configured properly.

Expected Result:

For Steps 1a- 1d, all TLS-Protected Servers shall be configured properly according to the requirements found in this CP.

17.4 End User Device Configurations

This section contains a procedure to ensure that the configurations for all the EUDs in the MA solution follow the requirements given in this CP.

Requirements being tested: MA-EU-1 through MA-EU-50, MA-RD-1 through MA-RD-4, MA-DM-9

Procedure Description:

1) For the EUD, verify in the policy the following:

   a) Ensure that, if the implementing organization's policy allows local storage of user data of classified information on the EUD, the EUDwill be treated as classified if it does not have a NSA-approved DAR. (MA-EU-1)

   b) Inspect the implementing organization's policy that EUDs which implement an NSA-approved DAR solution comply with handling requirements specified for the DAR solution. (MA-EU-2)

   c) Verify through policy that for EUDs which do not allow for local user storage that the EUD is treated as unclassified when powered down. (MA-EU-3)

   d) Verify the EUD does not allow split tunneling. (MA-EU-7)

   e) Ensure that the implementing organization's policy states that all Remote Access users must sign an organization-defined user agreement prior to using an EUD. (MA-EU-15)

   f) Verify that the implementing organization has a training program in place for Remote Access users operating an EUD. (MA-EU-16)

   g) Verify that the implementing organization has a user agreement for EUD users and also policies for each element within their user agreement document. (MA-EU-17)

   h) Ensure that the implementing organization's policy states that the EUD is dedicated for use within the MA Solution. (MA-EU-18)

   i) Ensure that the implementing organization's policy states that the EUD is to be remotely administered. (MA-EU-19)

   j) Ensure that the implementing organization's policy states that the EUDs will have their certificates revoked and resident image removed prior to disposal. (MA-EU-24)

k) Verify that the Security Administrator has an organizational security policy for the EUDs. (MA-DM-9)

2) For the EUD, perform the following:

a) Inspect the EUD configuration setting to verify that Firmware-Over-the-Air updates are disabled from the cellular carrier. (MA-EU-21)

b) Inspect the EUD configuration setting has incoming cellular services are disabled. (MA-EU-23)

c) Inspect the EUD configuration setting to verify that the wireless interfaces not passing through the VPN Client are disabled. (MA-EU-22)

d) Verify that Red network services do not transmit any classified data to the EUD until user authentication succeeds. (MA-EU-12, MA-EU-13)

e) Inspect the EUD's configuration to ensure that Global Positioning System and location services are disabled except for those authorized by the AO. (MA-EU-20)

3) For each EUD that directly connects to a Black network, perform the following:

a) Inspect the Outer VPN Client and Inner Encryption Clients on the EUD and verify that separate private key stores are used. (MA-EU-4)

b) Verify that the Inner and Outer VPN Clients on the EUD are implemented on separate IP stacks, and that the two IP stacks are not the IPv4 and IPv6 implementations on the same operating system. (MA-EU-5)

4) If the EUD is not remotely administrated, verify that the procedure given in MA-EU-6 is followed and/or is currently in place.

5) Verify that the procedures given in MA-EU-8, MA-EU-9, MA-EU-10, MA-EU-11, MA-EU-27, MA-EU-29, MA-EU-31 and MA-EU-32 are followed and/or currently in place.

6) Verify that the password length for Mobile Platform complies with MA-EU-25.

7) For Solutions that are using a Retransmission Device, perform the following:

a) Attempt to connect an unauthorized RD to the EUD to verify that the EUD will not connect to the RD. (MA-RD-1).

b) Ensure that the only connection between the EUD and the Mobile Access Solution is only via Wi-Fi or Ethernet. (MA-RD-2)

c) If the RD is using Wi-Fi, verify through configuration file that the Wi-Fi network is using WPA2 PSK or certificate-based authentication. (MA-RD-3)

d) Verify that the placement of the RD between the Outer VPN Gateway and the Inner Encryption Component. (MA-RD-4)

8) Verify the EUDs use a unique X.509 v3 device certificate, signed by the Outer CA for mutual authentication with Outer VPN Gateways. (MA-EU-33)

9) Verify TLS EUDs use a unique X.509 v3 device certificate, signed by either the Inner CA, or a unique X.509 v3 user certificate signed by an authorized enterprises service CA for mutual authentication with TLS-Protected Servers. (MA-EU-34)

10) Verify VPN EUDs use a unique X.509 v3 device certificate, signed by the Inner CA for mutual authentication with Inner VPN Gateways. (MA-EU-35)

11) Verify that, during provisioning:

a) All unnecessary keys are destroyed from the EUD secure key storage. (MA-EU-44)

b) All unnecessary X.509 certificates are removed from the EUD Trust Anchor Database. (MA-EU-45)

12) If applicable,

a) Confirm use of Domestic Cellular Service as a Black Transport Network.

b) Ensure the EUDs use an Access Point Name (APN) provided by a domestic cellular carrier private network. (MA-EU-36)

13) Verify the EUDs are configured for all IP traffic, with the exception of IKE, network address configuration, time synchronization, and name resolution traffic required to establish the IPsec tunnel, to flow through the IPsec VPN client. (MA-EU-37)

14) If applicable, verify the EUDs are configured for all IP traffic, with the exception of IKE, to flow through the IPsec VPN Client.

15) Verify the EUDs are configured as follows:

a) Maximum password life time shall be less than 181 days. (MA-EU-39)

b) Screen shall lock after three minutes of inactivity. (MA-EU-40)

c) Shall perform a wipe of all protected data after no more than 10 authentication failures. (MA-EU-41)

d) If feasible, display notifications shall be disabled while in a locked state. (MA-EU-46)

e) If feasible, USB mass storage shall be disabled. (MA-EU-47)

f) USB data transfer shall be disabled, if feasible. (MA-EU-48)

16) Ensure VPN protection is enabled across the EUD. (MA-EU-42).

17) Ensure a security policy is in place on EUDs specific to each RD and/or Government Private Wireless network to which the EUD is to be connected. (MA-EU-43)

18) Where feasible, ensure the EUDs use an Access Point Name (APN) provided by a domestic Cellular carrier Private Network when using Domestic Cellular Service as the Black Transport Network. (MA-EU-36)

19) Ensure the system software digital signatures are verified prior to the Application Processor system software is updated. (MA-EU-49)

20) Ensure application digital signatures are verified prior to installing new applications. (MA-EU-50).

Expected Result:

For steps 1-3, all EUDs shall be configured properly. For steps 4, a remotely administrated EUD shall only be rekeyed over the MA solution network prior to the expiration of keys. If this cannot be accomplished, the EUD must be re-provisioned. For Step 5, the implementing organization should have policies in place in order to address the requirements identified. For Step 6, Mobile Platform passwords shall be verified. For Step 7, an organization using a RD will ensure that the RD is configured in accordance with this CP. For steps 8-10, unique X.509 v3 certificates are used for each layer. For step 11, only keys and certificates required for operation are on the EUD. Step 12, all traffic flows through the IPsec VPN client, unless it is required to establish the IPsec tunnel. Step 13 - 20, the EUDs are configured in accordance with this CP.

17.5 RETRANSMISSION DEVICE CONFIGURATION

This section contains a procedure to ensure that the configurations for the RD in the MA solution follow the requirements given in this CP.

Requirements being tested: MA-RD-5 through MA-RD-26

Procedure Description:

1) If the RD is configured to be a Wi-Fi access point, then ensure that the following configuration is in place:

a) If the RD is using PSK, the PSK is using a length of at least 32 hexadecimal characters (or equivalent). (MA-RD-5)

b) The RD shall only permit connections to devices on a Media Access Control (MAC) white list. (MA-RD-6)

c) If the RD is using PSK, the PSK is not displayed on the RD. (MA-RD-7)

d) The SSID and MAC addresses of connected devices are not displayed on the RD. (MA-RD-8, MA-RD-9)

e) Broadcast of the SSID is disabled. (MA-RD-18)

f) Wi-Fi Protected Setup (WPS) is disabled. (MA-RD-12)

g) Traffic of multiple EUDs sharing the RD is separated. (MA-RD-17)

h) If using WPA Enterprise, then certificate used for authentication shall be different from the certificates used to authenticate the outer and inner tunnels. (MA-RD-26)

2) Verify that the Administrator password is not displayed on the RD. (MA-RD-10)

3) Verify that the RD can display the number of currently connected devices. (MA-RD-11)

4) Verify that the RD can only be administered using HTTPS. (MA-RD-13)

5) Verify that the RD is configured to limit the number of connected devices to the maximum required for the mission. (MA-RD-16).

6) Verify that the RD only permits charging on the USB ports and interfaces. (MA-RD-19)

7) Verify that connected EUDs are unable to access files stored on the RD. (MA-RD-20)

8) Verify that the default RD Administrator credentials have been changed. (MA-RD-15)

9) Verify that a user is required to authenticate with Administrator credentials prior to being able to perform the following:

a) Perform changes to the RD. (MA-RD-14)

b) Download logs or configuration files. (MA-RD-21)

c) Update firmware. (MA-RD-24)

10) Verify the RD will only allow firmware updates signed by the RD manufacturer. (MA-RD-22)

11) Verity the RD cannot boot into recovery mode. (MA-RD-23)

Expected Result: The RD is configured in accordance with this CP.

17.6 Inner And Outer VPN Component Configurations

This section contains a procedure to ensure that the configurations for the Inner and Outer VPN Components in the MA solution follow the requirements given in this CP.

Requirements being tested: MA-SR-2, MA-SR-3, MA-SR-4, MA-SR-5, MA-SR-9, MA-CR-1 through MA-CR-15, MA-IR-1 through MA-IR-5, MA-OR-1 through MA-OR-7, MA-DM-1 through MA-DM-8, MA-DM-11 through MA-DM-13, MA-DM-18

Procedure Description:

1) For the Inner and Outer VPN component in the solution, perform the following:

   a) Obtain the current configuration for the VPN Component.

   b) Verify that a unique device certificate is loaded with the corresponding CA signing certificate. (MA-CR-4)

   c) Verify that a device certificate from a CA included in the MA solution is listed in the configuration for authentication. (MA-CR-5)

   d) Ensure that the corresponding CA signing certificate and certificate revocation information are on the VPN Component. (MA-CR-6)

   e) Ensure that default accounts, passwords, community strings, and other default access control mechanisms for all components are changed or removed. (MA-SR-4)

   f) Ensure that all components are configured in accordance with local policy and applicable U.S. Government guidance, or, in the event of conflict between this CP and local policy, this CP takes precedence (MA-SR-5)

   g) Ensure that Inner Encryption components are not performing switching or routing for other Encryption Components (MA-SR-9)

   h) Verify that the requirements MA-CR-1, MA-CR-2, MA-CR-3, MA-CR-7, MA-CR-9, MA-CR-10 through MA-CR-14, are configured properly.

   i) Ensure that the time of day on the Inner Encryption Endpoints, Inner Firewall, and Red Management Services matches the current time. This should be within a small margin of error, to be determined by the AO. (MA-SR-2)

j) Ensure that the time of day on the Outer Gateway, Gray Firewall and Gray Management Services matches the current time. This should be within a small margin of error, to be determined by the AO. (MA-SR-3)

k) Verify that the VPN Components are configured to re-authenticate the identity of the VPN Components at the other end before rekeying the IKE SA. (MA-CR-15)

l) Verify that any Outer VPN Gateway in the solution is not configured to perform routing. (MA-OR-9)

2) For the Inner VPN component in the solution, use the configuration from 1a and perform the following:

a) Log into the Inner VPN component and verify that it is configured to use Tunnel or Transport mode IPsec with an associated IP Protocol (i.e. GRE). (MA-IR-1)

b) Log into the Inner VPN component and verify that the MTU (for IPv4) or the PMTU (for IPv6) has been configured to an appropriate size. (MA-IR-2)

c) Using a packet analyzer tool on the Inner VPN Gateway, verify that traffic leaving the external interface going to the Outer VPN Gateway is encrypted. (MA-IR-3)

d) Using a packet analyzer tool on the EUD, ensure that all traffic leaving the Inner VPN client is encrypted except for traffic otherwise identified in this CP as permissible to send unencrypted. (MA-IR-4)

e) Using a packet analyzer tool on the Inner VPN Gateway, verify that traffic coming through the external interface of the Inner VPN Gateway is decrypted. (MA-IR-5)

f) Verify that a separate LAN or VLAN is established on the Enterprise/Red network and using a packet sniffer, inspect traffic within the Enterprise/Red Network to ensure it is being used exclusively for all management of Inner Encryption Endpoints and solution components within the Red network. (MA-DM-3)

3) For each Outer VPN component in the solution, use the configuration from 1a and perform the following:

a) Log into the Outer VPN component and verify that it is configured to use Tunnel mode IPsec. (MA-OR-1)

b) Verify the requirements MA-OR-2, MA-OR-3, and MA-OR-4, have been properly configured.

c) Verify that a separate LAN or VLAN is established on the Enterprise/Red network and using a packet sniffer, inspect traffic within the Gray network to ensure it is being used exclusively for all

management of Outer VPN Gateway, Gray firewall and solution components within the Gray network. (MA-DM-4)

d) Using a packet analyzer tool on the EUD, ensure that all traffic leaving the Outer VPN client is encrypted except for traffic otherwise identified in this CP as permissible to send unencrypted. (MA-OR-5)

e) Using a packet analyzer tool on the Outer VPN Gateway, verify that traffic coming through the external interface of the Outer VPN Gateway is decrypted. (MA-OR-7)

4) For an EUD that uses VMs to separate Inner and Outer VPN clients, verify that the Outer VPN client is not installed on the host operating system. (MA-OR-6)

5) For all device administration, verify that requirements MA-DM-6, MA-DM-1, MA-DM-2, and MA-SR-8, MA-DM-18 are configured properly.

6) For each administration workstation, ensure the Security Administrator is required to authenticate to the component before being granted access. (MA-DM-7)

7) For each administration workstation, ensure the Security Administrator is required to authenticate to solution components using Suite B compliant certificates. (MA-DM-8)

8) Ensure that certificate signing requests are initiated by the Security Administrator as part of their initial keying within the solution. (MA-DM-11)

9) Ensure that devices use EST as detailed in RFC 7030 for certificate management. (MA-DM-12)

10) Ensure that the same Administration Workstation is not used to manage both Inner and Outer VPN Gateways. (MA-DM-13)

11) Ensure that requirement MA-DM-5 has been configured properly.

Expected Result:

For Steps 1-7, the Inner and Outer VPN Components should be configured properly according to the requirements found in this CP. For Steps 8-10, all VPN Component administration devices should be configured properly based upon the requirements of this CP. For Steps 11-12, all of the procedures have been followed or are in place.

17.7 Key Management

This section contains a procedure to ensure that key management capabilities for the MA solution follow the requirements given in this CP.

Requirements being tested: MA-KM-1 through MA-KM-49, MA-AU-36 through MA-AU-38, MA-PF-3

Procedure Description:

1) Perform the following to validate the correct deployment of CAs:

    a) ()For CAs, verify the configuration of the MA Solution to ensure that Outer CAs deliver services through either the Gray or Red networks; and, Inner CAs only deliver services through the Red network. (MA-KM-2, MA-KM-3)

    b) For CAs, verify that the Outer and Inner CAs are physically separate from one another. (MA-KM-4)

    c) For Locally-run CAs that operate on-line, verify the CAs utilize FIPS 140-2 Level 2 or higher Hardware Security Modules (HSMs) to protect the CAs' private signing keys. (MA-KM-12)

    d) For all CAs, verify that the CA does not have access to any MA Solution Component private keys. (MA-KM-11)

Expected Results: CAs are correctly deployed and in compliance with requirements MA-KM-1 through MA-KM-4, MA-KM-11 and MA-KM-12.

2) Perform the following to validate the structure of certificates issued by CAs:

    a) Obtain a sample set of test certificates issued to MA solution components.

    b) Verify the Distinguished Name in each certificate identifies a Non-Person Entity (NPE), unless that certificate is used in a TLS EUD where a user certificate is required. In this case, the certificate DN identifies a human user. (MA-KM-5)

    c) Verify the Key Usage extension in the each certificate only asserts "digitalSignature". (MA-KM-6)

    d) Verify the certificates are compliant with the data standard for Version 3 certificates defined in ITU-T Recommendation X.509. (MA-KM-7)

    e) Verify the certificates are compliant with IETF RFC 5280 profile requirements. (MA-KM-8)

    f) Verify the certificates are compliant with the key sizes and algorithms specified in Tables 9-11. (MA-KM-10)

Expected Results: The Certificate structure and content are compliant with requirements MA-KM-5 through KM-8 and MA-KM-10.

3) Perform the following to validate correct policy implementation as it relates to CAs and certificates issued by the CAs:

   a) Verify the CA has a Certificate Policy and a Certification Practices Statement (CPS) in place that is compliant with IETF RFC 3647, and that the CA operates in accordance with the policy and CPS. (MA-KM-13, MA-AU-36, MA-AU-37, MA-AU-38)

   b) Verify that the MA Solution policy states device authentication certificates issued by the CA, along with corresponding private keys, are considered Controlled Unclassified Information (CUI), and user private keys are classified to the level determined by the AO. (MA-KM-1, MA-KM-9)

Expected Results: CA policy exists and complies with requirements MA-KM-9 and MA-KM-13.

4) Perform the following steps to validate the certificate issuance capability of the MA solution:

   a) Verify that a physical environment is identified to initially load keys and certificates onto MA Solution Components, where the environment is certified to protect information at the highest classification level of the MA Solution red network. (MA-KM-14)

   b) Verify that the key and certificate provisioning process for MA Solution Components ensures private keys are never escrowed. (MA-KM-15)

   c) Generate a public/private key pair for the Outer VPN Component that complies with the key size and algorithm requirements in Tables 9-11. If the Component is capable of generating its own key pair, the key pair is to be generated on the Component. Else, the key pair is generated by a dedicated management workstation.

   d) Generate a certificate request for the Outer VPN Component, and ensure the request complies with PKCS#10.

   e) Submit the certificate request to the Outer CA, and verify that the CA returns a signed certificate using PKCS#7. (MA-KM-16)

   f) If the key pair was generated by a management workstation, install the certificate and private key using PKCS#12. If the key pair was generated by the VPN Component, install the signed certificate using PKCS#7. (MA-KM-17, MA-KM-18)

   g) Repeat steps 4c through 4f for each Inner Encryption Component of the MA Solution.

   h) If the MA Solution supports IETF RFC 7030 (Enrollment over Secure Transport (EST)), verify that the certificate request, response and installation process complies for MA Solution Components complies with EST. (MA-KM-19)

i) Verify that the certificate request and issuance processes comply with the Outer and Inner CAs' Certificate Policies and CPSs. (MA-KM-20, MA-KM-21)

j) For locally run CAs, verify the Certificate Policies and CPSs to ensure certificate issued by the CAs: 1) enforce unique Distinguished Names (DNs); 2) assert key usages as defined by MA-KM-5; and 3) assert a registered policy Object Identifier (OID).

k) For locally run CAs, examine the contents of a sample set of issued certificates to ensure that the certificates assert: 1) unique Distinguished Names (DNs); 2) key usages as defined by MA-KM-5; and 3) a registered policy OID. (MA-KM-22)

l) For all CAs, examine the contents of a sample set of issued certificates and ensure that at least one valid CRL Distribution Point (CDP) is asserted in the CDP extension of the certificates. (MA-KM-23)

m) For locally run CAs, ensure the validity periods asserted in certificates issued by the CAs do not exceed 14 months for MA End User Devices (EUDs). (MA-KM-24)

n) For locally run CAs, ensure the validity periods asserted in certificates issued by the CAs do not exceed 36 months for MA Solution Infrastructure Components. (MA-KM-25)

o) Verify that the Inner CAs can only issue certificates to Inner Encryption Components and Red Network Components. (MA-KM-26)

p) Verify that the Outer CAs can only issue certificates to Outer VPN Components and Gray Network Components. (MA-KM-27)()()

Expected Results:

For Step 4a, a physical environment exists to initially load keys and certificates onto MA Solution Components, where the environment is certified to protect information at the highest classification level of the MA Solution Red network.

For Step 4b, private keys for MA Solution Components cannot be escrowed.

For Steps 4c-4e, the certificate request/response process between the MA Solution Component and the CAs correctly implements PKCS#10 and PKCS#7.

For Step 4f, the key and certificate installation process correctly implements PKCS#12 or PKCS#7.

For Step 4g, same results as for steps 4c through 4f.

For Step 4h, the certificate request/response process between the MA Solution Component and the CAs correctly implements EST.

For Step 4i, the certificate request/response process complies with the CAs' Certificate Policies and CPSs.

For Step 4j-4n, the contents of certificates issued by the CAs comply with requirements MA-KM-22 through MA-KM-25.

For Step 4o, Inner CAs can only issue certificates to Inner Encryption Components and Red Network Components.

For Step 4p, Outer CAs can only issue certificates to Outer VPN Components and Gray Network Components.

For Step 4q, Enterprise Root CA shall issue certificates the Subordinate CAs for the Red and Gray networks respectively.

For Step 4r, the Subordinate CAs shall issue certificates for the inner and outer tunnels.

5) Perform the following steps to validate the certificate renewal and rekey capability of the MA solution:

   a) Verify that the certificate renew and rekey processes comply with the Outer and Inner CAs' Certificate Policies and CPSs. (MA-KM-31)

   b) Verify that the Outer and Inner CAs' Certificate Policies and CPSs require certificate renew and rekey be performed prior to a certificate expiring. Verify the Outer and Inner CAs' Certificate Policies and CPSs require an MA Solution Component go through the initial certificate issuance process if the certificate is expired. (MA-KM-30)

   c) Generate a new public/private key pair for the Outer VPN Component that complies with the key size and algorithm requirements in Tables 9-11. If the Component is capable of generating its own key pair, the key pair is to be generated on the Component. Else, the key pair is generated by a dedicated management workstation.

   d) Generate a certificate renew and rekey request for the Outer VPN Component, and ensure the request complies with PKCS#10.

   e) Submit the certificate request to the Outer CA, and verify that the CA returns a signed certificate using PKCS#7. (MA-KM-32)

   f) Repeat steps 5c through 5e for each Inner Encryption Component of the MA Solution.

g) If the MA Solution supports IETF RFC 7030 (Enrollment over Secure Transport (EST)), verify the certificate renew and rekey request, response and installation process complies for MA Solution Components complies with EST. (MA-KM-35)

Expected Results:

For Step 5a, the certificate renew and rekey request/response process complies with the CAs' Certificate Policies and CPSs.

For Step 5b, the CAs' Certificate Policies and CPSs require certificate renew and rekey to be performed prior to the certificate expiring. If the certificate is expired, the Certificate Policies and CPSs require the MA Solution Component go through the initial certificate issuance process.

For Steps 5c-5e, the certificate renew and rekey request/response process between the MA Solution Component and the CAs correctly implements PKCS#10 and PKCS#7.

For Step 5f, the key and certificate installation process for certificate renew and rekey correctly implements PKCS#12 or PKCS#7.

For Step 5g, same results as for steps 5c through 5f.

For Step 5h, the certificate renew and rekey request/response process between the MA Solution Component and the CAs correctly implements EST.

6) Perform the following steps to validate the certificate revocation and CDP capabilities of the MA solution:

a) Verify that the Outer and Inner CAs' Certificate Policies and CPSs define requirements and procedures for revoking MA Solution Component certificates, where certificate revocation is required when the binding between the subject information and public key within the certificate is no longer considered valid. (MA-KM-36)

b) Verify that the Outer and Inner CAs' Certificate Policies and CPSs define requirements and procedures for requesting the revocation of MA Solution Component certificates. (MA-KM-40)

c) For locally run CAs, verify the Outer and Inner CAs' Certificate Policies and CPSs define certificate revocation requirements and procedures for MA Solution Components that address: 1) response to a lost, stolen or compromised MA EUD; 2) removal of a revoked MA infrastructure device from the MA Solution network; 3) re-establishment of a MA Solution Component after certificate revocation is performed; 4) revocation of certificates when a MA EUD is considered compromised; and 5) revocation of

certificates if simultaneous use of the certificate is detected from different IP addresses. (MA-KM-41)

d) Verify that the Outer and Inner CAs has the capability to generate CRLs after certificate revocation functions are performed. (MA-KM-37)

e) Obtain CRLs from the Outer and Inner CAs and ensure their structures are compliant with the data standard for Version 2 CRLs defined in ITU-T Recommendation X.509, and with the CRL profile standard defined by IETF RFC 5280. (MA-KM-38, MA-KM-39)

f) Obtain CRLs from the Outer and Inner CAs and upload them onto the CDPs defined for the MA Solution. Depending on the MA Solution configuration, Outer CA CRLs can be uploaded onto Black and/or Outer CDPs; Inner CA CRLs can be uploaded onto Gray and/or Red CDPs.

g) Verify that MA Solution Components can access the CDPs and download the CRLs issued by the Outer and Inner CAs via HTTP. Outer VPN Components and Gray Management Service Components are able to access and download the CRL issued by the Outer CA; Inner Encryption Components and Red Management Service Components are able to access and download the CRL issued by the Inner CA. (MA-KM-42, MA-PF-3)

h) For Enterprise CAs, verify that the Certificate Policies and CPSs define requirements and procedures for publishing CRLs. (MA-KM-43)

i) For locally run CAs, verify that the Certificate Policies and CPSs define requirements and procedures for 1) publishing new CRLs at least once every 28 days; 2) creating a new CRL within one hour of a certificate being revoked; and 3) publishing a newly created CRL at least 7 days before the expiration of the current CRL. (MA-KM-44, MA-KM-45, MA-KM-47)

j) Verify the MA Solution has procedures defined to transfer new CRLs to MA Solution CDPs within 24 hours of the CRLs being created. (MA-KM-46)

k) For MA Solutions that support the On-Line Certificate Status Protocol (OCSP) to provide certificate revocation status information, verify the OCSP Servers are deployed on the Gray and Red networks to deliver OCSP responses in accordance with IETF RFC 6960. (MA-KM-48)

l) Generate an OCSP request from the Outer VPN Gateway and send the request to the OCSP Server operating in the Gray network.

m) Generate an OCSP response from the OCSP Server in the Gray network and deliver it to the Outer VPN Gateway.

n) Examine the OCSP Response, and verify that it is digitally signed and compliant with IETF RFC 6960. (MA-KM-49)

o) Repeat steps 6l-6n for all MA Solution Inner Encryption Components using an OCSP Server operating in the Red network. (MA-KM-49)

Expected Results:

For steps 6a-6c, the Certificate Policies and CPSs have requirements and procedures defined to satisfy requirements MA-KM-36, MA-KM-40 and MA-KM-41.

For steps 6d and 6e, the CAs are able to generate Version 2 CRLs that are compliant with ITU-T Recommendation X.509 and IETF RFC 5280.

For steps 6f and 6g, MA Solution Components successfully access and download CRLs from CDPs deployed in the Gray and Red networks of the MA Solution.

For steps 6h and 6i, the Certificate Policies and CPSs have requirements and procedures defined to satisfy requirements MA-KM-43 through MA-KM-45, and MA-KM-47.

For step 6j, procedures exist to transfer new CRLs to MA Solution CDPs within 24 hours of the CRLs being created. (MA-KM-46)

For steps 6k through 6o, OCSP Servers are correctly deployed in the Gray and Red networks and issue digitally signed OCSP responses compliant with IETF RFC 6960 to MA Solution Components. (MA-KM-48 and MA-KM-49)

17.8 Solution Filtering Configurations

This section contains a procedure to ensure that the filtering configurations for all the MA solution follow the requirements given in this CP.

Requirements being tested: MA-PF-1 through MA-PF-2, MA-PF- 4 through MA-PF-16

Procedure Description:

1) Perform the following steps on the each of the Solution Components:

a) Log into the component.

b) Verify through the configuration file that network interfaces are restricted to the smallest address range, ports, and protocols (MA-PF-1).

c) Verify through the configuration file that all unused network interfaces are disabled (MA-PF-2).

2) For the Outer VPN Gateway perform the following:

    a) Obtain the current configuration for the Outer VPN Gateway.

    b) Verify that the requirements MA-PF-4, MA-PF-7 or MA-PF-8, , MA-PF-9 through MA-PF-12 are met.

3) For the Inner VPN Gateway perform the following:

    a) Obtain the current configuration for the Inner VPN Gateway.

    b) Verify the requirements MA-PF-5.

4) Establish a connection from the EUD to the Red network.

    a) Using a protocol analyzer on the Outer firewall, observe inbound and outbound traffic on the Outer firewall.

    b) Verify that the only protocols that are allowed through are IKE, ESP, and control plan protocols as specified in MA-PF-13.

5) For the Inner firewall perform the following:

    a) Log into the Inner firewall.

    b) Obtain the configuration file.

    c) Verify that the Inner firewall has a whitelist for all Inner Encryption Endpoints (MA-PF-6).

6) For the EUDs consisting of a single computing platform

    a) Verify there is no ingress or egress of Certificate Revocation traffic (OCSP queries, HTTP GET to CDPs) on the Black interface. (MA-PF-14)

    b) Verify there is no ingress or egress of Name Resolution traffic (e.g. DNS query/response) on the Black interface. (MA-PF-15)

    c) Verify there is no ingress and egress of NTP traffic on the Black interface. (MA-PF-16)

Expected Result:

For Step 1, the Solution components network interfaces are configured properly. For Step 2- 4, the Outer, Inner VPN Gateway, and Outer firewall are only allowing the necessary protocols. For Step 5, verify that the Inner firewall is configured correctly. For Step 6, verify there is no

Certificate Revocation, name resolution, or NTP traffic between the EUDs and the Black network.

17.9 Configuration Change Detection

This section contains a procedure to ensure that changes made to any of the MA Solution configurations are detected by the Configuration Change Detection tool.

Requirements being tested: MA-CM-1 through MA-CM-3

Procedure Description:

1) The following shall be performed for each of the Solution components within this CP.

   a) Log into the Solution components (Outer firewall, Outer VPN Gateway, Gray firewall, Gray Management Services, Inner Encryption Endpoints, Red Management Services, EUD, and Retransmission Device (if applicable)).

   b) Compare the current version of the Solution Component's configuration with the stored baseline and ensure the current version matches the stored configuration. (MA-CM-1)

   c) Make a change to the configuration, preferably something that is not fundamental to the security of the MA solution.

   d) Look in the audit log to determine if a log entry has been generated about the configuration change and that the changes from 1c are recorded. (MA-CM-2).

   e) Inspect the monitoring service to verify that the service has detected a change in configuration. (MA-CM-3)

Expected Result:

The Auditor will validate the baseline configuration was stored in Step 1b. In Step 1d, there should be a log entry created for the configuration change in the audit log including the actual configuration change. Lastly if there was a configuration change, a monitoring service will detect a change in the configuration.

17.10 Continuous Monitoring

This section contains procedures for ensuring traffic is monitored for and alerts generated for potential unauthorized/malicious traffic. It also contains procedures for ensuring a SIEM is in place to collect logs and that it is configured correctly.

Requirements being tested: MA-MR-1 through MA-MR-18

Procedure Description:

1) Ensure that an IDS/IPS is deployed to monitor traffic in at least one of three locations (MA-MR-1 through MA-MR-6):
    a) Between the Outer firewall and Outer VPN Gateway (M1)
    b) Between the Outer VPN Gateway and the Gray firewall (M2)
    c) On the internal side of the Inner firewall (M3)
2) Ensure that each IDS/IPS in the solution is configured to send alerts to the Security Administrator, and, where possible, block malicious traffic. (MA-MR-7, MA-MR-8)
3) Ensure that each IDS/IPS in the solution is configured with rules that will generate alerts and, where possible, block traffic for any unauthorized source and destination IP addresses (MA-MR-9 through MA-MR-12).
4) Ensure that an SIEM is implemented (MA-MR-13 – MA-MR-16).
    a) Ensure the SIEM is implemented in the Gray network.
    b) Otherwise, if the SIEM is implemented within the Enterprise/Red network, ensure devices are configured to push events to an Enterprise/Red SIEM and through an AO-approved one-way tap.
    c) Send packets expected to be blocked by the Outer VPN Gateway or Gray firewall. Ensure the SIEM sends alerts to the Auditor when anomalous behavior such as this is detected.
    d) Ensure that logs from the Outer VPN Gateway Gray firewall and any other components located within the Gray Management Services are collected on the Gray SIEM.
    e) Ensure these logs are encrypted with TLS, SSHv2, or IPSEC.
5) Ensure that any one-way taps are deployed as per MA-MR-17 – MA-MR-18.
    a) Ensure that any one-way taps deployed as part of the solution are approved for use by the AO.
    b) Ensure that the SIEM implemented at the Red level that collects black and/or gray monitoring data sent through any one-way tap is deployed in an enclave isolated from the Red/Enterprise Network.
    c) Ensure that monitoring data flowing from M2 and/or M1 can transit to the SIEM if implemented at the Red level.
    d) Attempt to send other data through the one-way taps to determine if this data is blocked.

Expected Result:

For Steps 1 – 3, an IDS or IPS is in place to monitor, block where possible, and send alerts as appropriate. For Steps 4 and 5, an SIEM shall be implemented either in the Gray network or the Red/Enterprise network via one-way taps, as approved by the AO and only monitoring data will be able to transit through these taps.

17.11 AUDIT

This section contains procedures for ensuring audit events are detected, the proper information is logged for each event, and there is a procedure detailed in the CPS documentation for auditing each CA device.

Requirements being tested: MA-DM-14, MA-DM-15, MA-AU-1 through MA-AU-22, MA-AU-29 through MA-AU-35, MA-DM-10, MA-DM-16, MA-DM-17

Procedure Description:

1) Examples for testing the ability of each MA Component to audit and log audit events specified in the CP are given below. Verify that for each event logged, the applicable data regarding the event is recorded for the log entry in accordance with Section 13.13.

    a) All actions performed by a user with super-user privileges (auditor, administrator, etc.) and any escalation of user privileges. (MA-AU-12, MA-AU-13)\

        i) Log in as an administrator to the Solution Infrastructure Components or a EUD.

        ii) Perform a variety of administrator actions on the Solution Infrastructure Components or EUD.

        iii) Verify that a log entry was created for each action taken in Step ii that required super-user privileges and also states the escalation of privileges.

        iv) If performing an action on anEUD, verify that the EUD is generating logs and sends the logs to the central SIEM. (MA-DM-10)

        v) Revert back to the baseline configuration, eliminating the changes made in Step ii.

        vi) Repeat the above with the Auditor role.

    b) Changes to time. (MA-AU-15)

        i) Log in as a Security Administrator to the Solution Infrastructure Components.

        ii) Modify the system time on the Solution Infrastructure Components by at least 1 hour.

iii) Verify that a log entry was created due to the change in system time and by whom.

iv) Revert the system time back to the accurate time of day.

c) Log into and out of the MA Solution as a normal user and send traffic to the Red Network. Then log into the central SIEM as an Auditor, and inspect the audit entry for the following: MA-DM-14, MA-DM-15.

i) Verify that the log on as a normal user is logged and has an identifiable code for the type of event. (MA-AU-10, MA-AU-18)

ii) Verify that the log entry identifies the subject accessing the solution. (MA-AU-20)

iii) Verify that the log entry identifies the event. (MA-AU-17)

iv) Verify that the log entry includes the time, date, and the time zone offset. (MA-AU-16)

d) Establish and terminate a VPN tunnel. Verify in the logs, that these two events were logged. (MA-AU-1, MA-AU-3, MA-AU-5, MA-AU-7)

i) Establish and terminate a TLS connection. Verify in the logs, that these two events were logged. (MA-AU-2, MA-AU-4, MA-AU-6, MA-AU-8)

e) Log into a Solution Infrastructure Components as a Security Administrator and delete previously recorded audit log. Verify the log recorded this deletion. (MA-AU-9)

f) As the Certificate Authority Administrator, log into the audit log and attempt to delete a log entry. Verify this action is recorded with a failure code. (MA-AU-11, MA-AU-19)

g) Verify a log entry was created for the attempted unauthorized action.

2) Verify the source address, user, and for role-based events, role identity for all audit log entries is recorded. (MA-AU-21, MA-AU-22)

3) Verify that all logs forwarded to a SIEM on a Gray Management network are configured to be encrypted while in transit using SSHv2, IPSEC, or TLS with the appropriate Suite B algorithm supported by the solution. (MA-DM-16)

4) Verify that all logs forwarded to a SIEM on a Red Management network are configured to be encrypted while in transit using SSHv2, IPSEC, or TLS with the appropriate Suite B algorithm supported by the solution. (MA-DM-17)

5) Verify that the procedure MA-AU-35 is currently in place by the implementing organization and are followed.

6) Verify that the Outer VPN Gateway and Inner Encryption Components log the failure to pull the CRL from the Inner or Outer CDP. (MA-AU-29, MA-AU-30)

   a) CDP Servers shall remove all CRLs.

   b) Outer VPN Gateways and Inner Encryption Components shall attempt to pull the CRL from their respective CDPs**.**

   c) Review the Outer VPN Gateway and Inner Encryption Components audit logs to verify that a log report is generated from failure to pull the CRL.

7) Verify that the Outer VPN Gateway and Inner Encryption Components log if the version of the CRL on the Inner or Outer CDP is older than the current cached CRL. (MA-AU-31, MA-AU-32)

   a) Load the CDPs with CRLs that are older than the current cached CRLs on the Outer VPN Gateway and Inner Encryption Components.

   b) Have the Outer VPN Gateway and Inner Encryption Components attempt to pull the CRLs.

   c) Review the Outer VPN Gateway and Inner Encryption Components audit logs to verify that a log report is generated.

8) Verify that the Outer VPN Gateway and Inner Encryption Components log if signature validation of the CRL on the Inner or Outer CDP fails. (MA-AU-33, MA-AU-34)

   a) Load the CDPs with CRLs that contain an invalid signature.

   b) Have the Outer VPN Gateway and Inner Encryption Components pull the CRLs.

   c) Review the Outer VPN Gateway and Inner Encryption Components audit logs to verify that a log report is generated due to an invalid CRL signature.

9) For all Solution components, install approved certificates, generated by the approved CA, and configure the solution so that components use the certificates for authentication.

   a) Verify an entry to the Audit log has been created due to certificate loading and generation. (MA-AU-14)

   b) Initiate a revocation of certificates for the Solution components.

   c) Verify that an entry in the audit log has been created due to certificate revocation. (MA-AU-14)

Expected Result:

For Step 1, all occurrences of auditable events given should generate an entry in the audit log. For Step 2, the source address should be the MA Components' loopback address. For Steps 3-4, all logs forwarded on Red Management and Gray Management networks should be encrypted with the appropriate protocols. For Step 5, the procedure is followed and is in place. For Step 6-8, there should be an audit log entry created for each requirement. For Step 9, a log should be generated for generation and revocation of certificates.

17.12 EUD With Multiple Connections

This section contains a procedure to ensure that only one IPsec or TLS connection is allowed for the inner layer of encryption per EUD and that no other connections are permitted.

Requirements being tested: MA-AU-23 through MA-AU-28

Procedure Description:

1) For a IPsec connection, ensure that the EUD performs the following steps:
   a) The administrator will install the same device certificates on two EUDs.
   b) The administrator will authenticate to a Red network. At the same time, the Auditor will be reviewing the logs and detect that the same device certificate is coming from two different devices. (MA-AU-23)
   c) The Auditor will alert the Certificate Authority Administrator to revoke the certificates and provide an updated Certification Revocation List to the Security Administrator. (MA-AU-25)
   d) Once the Security Administrator receives notification from the Certificate Authority Administrator, the Security Administrator will drop both sessions. (MA-AU-27)
2) For TLS connection, ensure that the EUD performs the following steps:
   a) The administrator will install the same device certificates on two EUDs.
   b) The administrator will authenticate to a Red network. At the same time, the Auditor will be reviewing the logs and detect that the same device certificate is coming from two different devices. (MA-AU-24)
   c) The Auditor will alert the Certificate Authority Administrator to revoke the certificates and provide an updated Certification Revocation List to the Security Administrator. (MA-AU-26)
   d) Once the Security Administrator receives notification from the Certificate Authority Administrator, the Security Administrator will drop both sessions. (MA-AU-28)

Expected Result:

The same device certificate cannot be used for two devices. All results are expected to be pass/fail.

17.13 Incident Reporting Guidance

This section ensures that procedures are followed regarding incident reporting to NSA in the event a solution owner identifies a security incident which affects the solution.

Requirements being tested: MA-RP-1 through MA-RP-16

Procedure Description:

1) Verify that the procedures given in MA-RP-1 through MA-RP-16 were/are followed and are currently in place.

Expected Results:

For Step 1, all of these procedures have been followed or are in place.

17.14 Implementation of Guidance

This section ensures that there are procedures in place and/or that procedures were followed regarding the procurement of products and use of the MA solution. It also ensures the personnel are in place to manage and administer this solution following the guidelines given in the CP.

Requirements being tested: MA-GD-1 through MA-GD-41, MA-SR-6

Procedure Description:

1) Verify the procedures for obtaining virus signature updates as required by local agency policy and the AO were/are followed and/or are in place. (MA-SR-9)
2) Verify the procedures given in MA-GD-1 through MA-GD-8, and MA-GD-17 through MA-GD-30 were/are followed and/or are currently in place.
3) Verify that the solution owner understands that he/she shall allow and fully cooperate with an NSA-ordered IA compliance audit of this solution implementation. (MA-GD-9)
4) Verify that the AO are aware that a compliance audit will be conducted every year. (MA-GD-10)
5) Verify that the AO is aware that they shall receive the results of the compliance audit and are responsible for reviewing the completed audit. (MA-GD-11)

6) Verify that the customer is aware that when they are interested in registering their solution against this CP that NSA must grant them an approval prior to the AO authorizing the solution for operation. (MA-GD-12)

7) Verify that the customer completes and submit the compliance matrix to their AO. (MA-GD-13)

8) Verify that the customer is aware that registration and re-registration against this CP includes a submission of this CP registration forms and compliance matrix to NSA. (MA-GD-14)

9) Verify that the customer is aware that when a new MA CP is published by the NSA, the AO will comply against this new CP within 6 months. (MA-GD-15)

10) Verify that the solution owner and AO are aware that they shall provide updated solution information to NSA on a yearly basis. (MA-GD-16)

11) Verify that the personnel requirements given in MA-GD-31 through MA-GD-41 are met by the personnel supporting this implementation of the MA solution.

Expected Result:

For steps 1-10, all of these procedures have been followed or are in place.

17.15 Solution Functionality

This section contains a procedure for ensuring the implementing organization complies with the testing requirements.

Requirements being tested: MA-TR-1

Procedure Description:

1) The implementing organization's AO will inspect the test report in order to ensure all testing requirements have been met. (MA-TR-1)

Expected Result:

The report will ensure that the implementing organization complies with the MA Solution.

APPENDIX A. GLOSSARY OF TERMS

Authorization (To Operate) – The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls. (NIST SP 800-37)

Authorization Boundary – All components of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems, to which the information system is connected.

Authorizing Official – A senior (Federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

Authorizing Official Designated Representative – An organizational official acting on behalf of an authorizing official in carrying out and coordinating the required activities associated with security authorization.

Authorization Package – A security package of documents consisting of the security control assessment that provides the authorizing official with essential information needed to make a risk-based decision on whether to authorize operation of an information system or a designated set of common controls.

Assurance – Measure of confidence that the security features, practices, procedures, and architecture of an information system accurately mediates and enforces the security policy. (CNSSI 4009)

Audit – The activity of monitoring the operation of a product from within the product. It includes monitoring of a product for a set of pre-determined events. Each audit event may indicate rogue behavior, or a condition that is detrimental to security, or provide necessary forensics to identify the source of rogue behavior.

Audit Log – A chronological record of the audit events that have been deemed critical to security. The audit log can be used to identify potentially malicious activity that may further identify the source of an attack, as well as potential vulnerabilities where additional countermeasures or corrective actions are required.

Availability – Ensuring timely and reliable access to and use of information. (NIST SP 800-37).

Black Box Testing – Testing the functionality of a component of the solution, such that testing is limited to the subset of functionality that is available from the external interfaces of the box during its normal

operational configuration without any additional privileges (such as given to the Security Administrator or Auditor).

Black Network – A network that contains classified data that has been encrypted twice. (See Section 4.1.3)

CP – The set of guidance provided by NSA that describes recommended approaches to composing COTS components to protect classified information for a particular class of security problem. CP instantiations are built using products selected from the CSfC Components List.

Central Management Site – A site within a MA solution that is responsible for remotely managing the solution components located at other sites (see Section 4.2.3.2).

Certificate Authority (CA) – An authority trusted by one or more users to create and assign certificates. (ISO9594-8)

Certificate Policy (CP) – A named set of rules that indicate the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular CP might indicate applicability of a type of certificate to the authentication of parties engaging in business-to-business transactions for the trading of goods or services within a given price range. (IETF RFC 3647)

Committee on National Security Systems Policy No. 15 (CNSSP-15) – Policy specifies which public standards may be used for cryptographic protocol and algorithm interoperability to protect National Security Systems (NSS).

Confidentiality – Assurance that the data stored in, processed by, or transmitted by the system are protected against unauthorized disclosure, and confidence that only the appropriate set of individuals or organizations would be provided the information.

Control Plane Protocol – A routing, signaling, or similar protocol whose endpoints are network infrastructure devices such as VPN Gateways or routers. Control plane protocols carry neither user data nor management traffic.

CRL Distribution Point (CDP) – A web server that hosts a copy of a CRL issued by a CA for VPN Components to download (see Section 9.1).

Cross Domain Solution (CDS) – A form of controlled interface that provides the ability to manually and/or automatically access and/or transfer information between different security domains. (CNSSI 4009)

Data Plane Protocol – A protocol that carries the data being transferred through the solution.

End User Device (EUD) – A form-factor agnostic component of the Mobile Access solution that can include a mobile phone, tablet, or laptop computer. EUDs can be composed of multiple comments to provide physical separation between layers of encryption (see Section 4.2.1 for explanation of detailed differences between VPN EUD and TLS EUD solution design options).

Enterprise/Red Network – A network that contains unencrypted classified data and can contain singly encrypted gray data (see Section 4.1.1).

External Interface – The interface of the Outer VPN Gateway that connects to the internal interface of the Outer firewall.

Federal Information Processing Standards (FIPS) – A set of standards that describe the handling and processing of information within governmental agencies.

Gray Box Testing – The ability to test functionality within a component of the solution, such that full management privileges are granted (i.e. knowing passwords for security administrator and Auditor and access to the capabilities associated with those privileges). In addition, the use of any and all testing equipment and/or testing software used inside and outside the developed solution is available.

Gray Network – A network that contains classified data that has been encrypted once (see Section 4.1.2).

Gray Firewall – A stateful traffic filtering firewall placed on the Gray network to provide filtering of ports, protocols, and IP addresses to ensure traffic reaches the correct Inner Encryption Endpoint or is dropped.

Internal Interface – The interface on a VPN Gateway or Inner Encryption Component that connects to the inner network (i.e., the Gray network on the Outer VPN Gateway or the Red network on the Inner Encryption Component).

Locally Managed Device – A device that is being managed by the direct connection of the Administration Workstation to the device in a hardwired fashion (such as a console cable).

Malicious – Any unauthorized events that are either unexplained or in any way indicate adversary activity.

Management Plane Protocol – A protocol that carries either traffic between a system administrator and a component being managed, or log messages from a solution component to a SIEM or similar repository.

Protection Profile – A document used as part of the certification process according to the Common Criteria. As the generic form of a security target, it is typically created by a user or user community and provides an implementation independent specification of information assurance security requirements.

Public Key Infrastructure (PKI) – Framework established to issue, maintain, and revoke public key certificates.

Remotely Managed Device – A device that is being managed by any other method besides that given in the definition of a Locally Managed Device.

Security Level – The combination of classification level, list of compartments, dissemination controls, and other controls applied to the information within a network.

Split-tunneling – Allows network traffic to egress through a path other then the established VPN tunnel (either on the same interface or another network interface). Split tunneling is explicitly prohibited in MA CP compliant configurations (see MA-OR-2 and MA-EU-7).

SRTP Client – A component on the EUD that facilitates encryption for voice communications.

TLS Client – A component on a TLS EUD that can provides the Inner layer of DIT encryption.

TLS Component – Refers to both TLS Clients and TLS-Protected Servers.

VPN Client – A VPN application installed on an EUD.

VPN Component – The term used to refer to VPN Gateways and VPN Clients.

VPN Gateway – A VPN device physically located within the VPN infrastructure.

VPN Infrastructure – Physically protected in a secure facility and includes Inner and Outer VPN Gateways, Certificate Authorities, and Administration Workstations, but does not include EUDs.

APPENDIX B. ACRONYMS

Acronym	Definition
AES	Advanced Encryption Standard
AO	Authorizing Official
APN	Access Point Name
ARP	Address Resolution Protocol
BIOS	Basic Input/Output System
BGP	Border Gateway Protocol
CA	Certificate Authority
CAA	Certificate Authority Administrator
CDP	CRL Distribution Point
CDS	Cross Domain Solution
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
CNSSP	Committee on National Security Systems Policy
COTS	Commercial Off-the-Shelf
CP	Certificate Policy
CP	Capability Package
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSfC	Commercial Solutions for Classified
CUI	Controlled Unclassified Information
DAR	Data-At-Rest
DDoS	Distributed Denial of Service
DH	Diffie-Hellman
DHCP	Dynamic Host Configuration Protocol
DHS	Department of Homeland Security
DM	Device Management
DN	Domain Name
DNS	Domain Name System
DOD	Department of Defense
DoE	Department of Energy
DoS	Denial of Service
DSA	Digital Signature Algorithm
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
ESP	Encapsulating Security Payload
EST	Enrollment Over Secure Transport
EUD	End User Device
FDE	Full Disk Encryption
FIPS	Federal Information Processing Standards

Acronym	Definition
FOTA	Firmware Over The Air
GOTS	Government Off-the-Shelf
GRE	Generic Routing Encapsulation
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IAD	Information Assurance Directorate
IAVA	Information Assurance Vulnerability Alert
ICMP	Internet Control Message Protocol
ICT	Information Communication Technology
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IKE	Internet Key Exchange
IP	Internet Protocol
IPS	Intrusion Prevention System
IPsec	Internet Protocol Security
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
IS-IS	Intermediate System to Intermediate System
KM	Key Management
MA	Mobile Access
MDF	Mobile Device Fundamentals
MDM	Mobile Device Manager
MOA	Memorandum of Agreement
MLD	Multicast Listener Discovery
MTU	Maximum Transmission Unit
NDP	Neighbor Discovery Protocol
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NPE	Non Person Entity
NSA	National Security Agency
NSS	National Security Systems
NTP	Network Time Protocol
O	Objective
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OPSEC	Operational Security
OS	Operating System
OSI	Open System Interconnection
OSPF	Open Shortest Path First
PKCS	Public Key Cryptographic Standard

Acronym	Definition
PKI	Public Key Infrastructure
PMTU	Path Maximum Transmission Unit
POC	Point of Contact
PTP	Precision Time Protocol
RD	Retransmission Device
RFC	Request for Comment
RIP	Routing Information Protocol
RSA	Rivest Shamir Adelman algorithm
S3	Secure Sharing Suite
SA	Security Association
SCRM	Supply Chain Risk Management
SDES	Session Description Protocol Security Descriptions
SHA	Secure Hash Algorithm
SIEM	Security Information and Event Manager
SIP	Session Initiation Protocol
SIPRNet	Secret Internet Protocol Router Network
SP	Service Packs
SRTP	Secure Real-Time Protocol
SSH	Secure Shell
SSHv2	Secure Shell Version 2
T	Threshold
T&E	Test and Evaluation
TCP	Transmission Control Protocol
TFFW	Traffic Filtering Firewall
TLS	Transport Layer Security
UDP	User Datagram Protocol
URL	Uniform Resource Locator
VDI	Virtual Desktop Infrastructure
VoIP	Voice over Internet Protocol
VM	Virtual Machine
VPN	Virtual Private Network
WLAN	Wireless Local Area Network
WPA2	Wi-Fi Protected Access II

APPENDIX C. REFERENCES

CNSSI 1300	*CNSSI 1300, National Security Systems Public Key Infrastructure X.509 Certificate Policy*	October 2009
CNSSI 4009	*CNSSI 4009, National Information Assurance (IA) Glossary Committee for National Security Systems.* http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf	April 2010
CNSSP 15	*CNSS Policy (CNSSP) Number 15, National Information Assurance Policy on the Use of Public Standards for the Secure Sharing of Information Among National Security Systems Committee for National Security Systems*	March 2010
CNSSD 505	*CNSS Directive (CNSSD) Number 505, Supply Chain Risk Management (SCRM)*	March 2012
FIPS 140	*Federal Information Processing Standard 140, Security Requirements For Cryptographic Modules National Institute for Standards and Technology FIPS Publication* http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf	May 2001
FIPS 180	*Federal Information Processing Standard 180-4, Secure Hash Standard (SHS)*	March 2012
FIPS 186	*Federal Information Processing Standard 186-4, Digital Signature Standard (DSS)*	July 2013
FIPS 197	*Federal Information Processing Standard 197, Advanced Encryption Standard (AES)*	November 2001
FIPS 201	*Federal Information Processing Standard 201, Personal Identity Verification (PIV) of Federal Employees and Contractors National Institute for Standards and Technology FIPS Publication* http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf	March 2006
IPsec VPN Client PP	*Protection Profile for IPsec Virtual Private Network (VPN) Clients*. http://www.niap-ccevs.org/pp	January 2012
NSA Suite B	*NSA Guidance on Suite B Cryptography (including the Secure Sharing Suite (S3))*. http://www.nsa.gov/ia/programs/ suiteb_cryptography/index.shtml	November 2010
RFC 2409	*IETF RFC 2409 The Internet Key Exchange (IKE)*. D. Harkins and D. Carrel.	November 1998
RFC 3647	*IETF RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework* Internet Engineering Task Force	November 2003
RFC 3711	*IETF RFC 3711 The Secure Real-Time Transport Protocol (SRTP).* M. Baugher and D. McGrew.	March 2004
RFC 4252	*IETF RFC 4252 The Secure Shell (SSH) Authentication Protocol*. T. Ylonen and C. Lonvick.	January 2006

RFC 4253	*IETF RFC 4253 The Secure Shell (SSH) Transport Layer Protocol*. T. Ylonen and C. Lonvick.	January 2006
RFC 4254	*IETF RFC 4254 The Secure Shell (SSH) Connection Protocol*. T. Ylonen and C. Lonvick.	January 2006
RFC 4256	*IETF RFC 4256 Generic Message Exchange Authentication for the Secure Shell Protocol (SSH)*. F. Cusack and M. Forssen.	January 2006
RFC 4302	*IETF RFC 4302 IP Authentication Header*. S. Kent	December 2005
RFC 4303	*IETF RFC 4303 IP Encapsulating Security Payload*. S. Kent	December 2005
RFC 4307	*IETF RFC 4307 Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)*. J. Schiller	December 2005
RFC 4308	*IETF RFC 4308 Cryptographic Suites for IPsec*. P. Hoffman	December 2005
RFC 4492	*IETF RFC 4492 Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS).* S. Blake-Wilson, N. Bolyard, V. Gupta, C. Hawk Corriente, B. Moeller, and Ruhr-Uni Bochum.	May 2006
RFC 4754	*IETF RFC 4754 IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA)*. D. Fu and J. Solinas.	January 2007
RFC 5246	*IETF RFC 5246 The Transport Layer Security (TLS) Protocol Version 1.2*. T. Dierks and E. Rescorla.	August 2008
RFC 5280	*IETF RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. D. Cooper, et. al.	May 2008
RFC 5759	*IETF RFC 5759 Suite B Certificate and Certificate Revocation List (CRL) Profile*. J. Solinas and L. Zieglar.	January 2010
RFC 5996	*IETF RFC 5996 Internet Key Exchange Protocol Version 2 (IKEv2)*. C. Kaufman, et. al.	September 2010
RFC 6188	*IETF RFC 6188 The Use of AES 192 and AES 256 in Secure RTP.* D. McGrew.	March 2011
RFC 6239	*IETF RFC 6239 Suite B Cryptographic Suites for Secure Shell (SSH)*. K. Igoe.	May 2011
RFC 6379	*IETF RFC 6379 Suite B Cryptographic Suites for IPsec*. L. Law and J. Solinas.	October 2011
RFC 6380	*IETF RFC 6380 Suite B Profile for Internet Protocol Security (IPsec)*. K. Burgin and M. Peck.	October 2011
RFC 6460	*IETF RFC 6460 Suite B Profile for Transport Layer Security (TLS)*. M. Salter and R. Housley.	January 2012
RFC 6818	*IETF RFC 6818 Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. P. Yee	January 2013
RFC 7030	*IETF RFC 7030 Enrollment over Secure Transport*. M. Pritikin, P. Yee, and D. Harkins.	October 2013

SP 800-53	*NIST Special Publication 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations*. Joint Task Force Transformation Initiative.	April 2013
SP 800-56A	*NIST Special Publication 800-56A Rev. 2, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*. E. Barker, et. al.	May 2013
SP 800-56B	*NIST Special Publication 800-56B, Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography*. E. Barker, et. al.	August 2009
SP 800-56C	*NIST Special Publication 800-56C, Recommendation for Key Derivation through Extraction-then-Expansion*. L. Chen.	November 2011
SP 800-131A	*NIST Special Publication 800-131A, Recommendation for Transitioning of Cryptographic Algorithms and Key Lengths*. E. Barker.	January 2011
SP 800-147	*NIST Special Publication 800-147, BIOS Protection Guidelines*. D. Cooper, et. al.	April 2011

APPENDIX D. END USER DEVICE IMPLEMENTATION NOTES

Virtual Private Network (VPN) End User Devices (EUDs):

The VPN EUD can be set up using a Computing Device with the user's applications, an Inner VPN Component, and an Outer VPN Component. The Inner VPN Component is a VPN client residing on the same computing device as the user applications. The Outer VPN Component can be a VPN Gateway from the VPN Gateway section of the CSfC Components List (as shown in Figure D-1) or be a VPN Client on the same Computing Device as the user applications (as shown in Figure D-2). If all components are on the same device, virtual machines will be required to provide separate IP stacks for the Inner and Outer VPN Clients as noted in Figure D-2. A retransmission device will also be required in this case, unless, as noted in Section 4.1.3, the connection is to a Wired Network, Domestic Cellular Network, Government Private Wireless Network or a Government Private Cellular network. See Figure D-3.

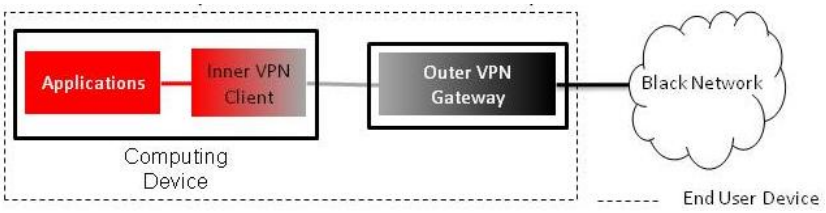

Figure D-1. VPN EUD with Inner VPN Client and Separate Outer VPN Gateway

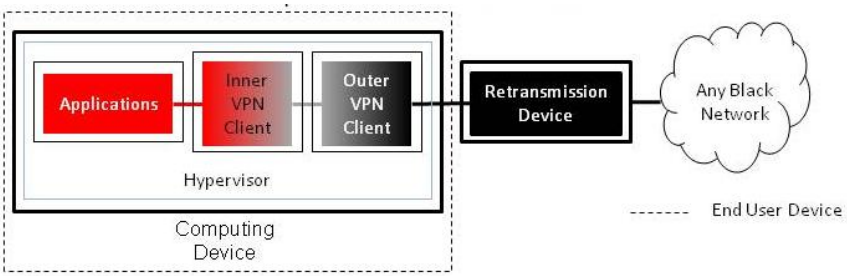

Figure D-2. VPN EUD with Inner and Outer VPN Clients in Separate Virtual Machines with Retransmission Device

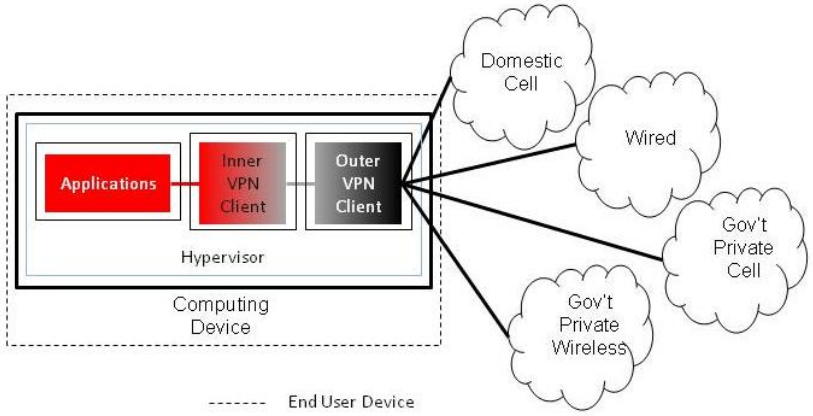

Figure D-3. VPN EUD with Inner and Outer VPN Clients in Separate Virtual Machines without Retransmission Device

Transport Layer Security (TLS) End User Devices:

The TLS EUDs can be set up using up to two separate components. These components consist of the Computing Device and the VPN Component. The Computing Device sends and receives classified data. The Outer VPN Component is either a VPN Gateway or a VPN Client. Outer VPN Gateways are always physically separate from the Computing Device and are selected from the IPsec VPN Gateway section of the CSfC Components List. VPN Clients are selected from the IPSec VPN Client section of the CSfC Components List. The Inner layer of encryption is always provided by an Application on the Computing Device which terminates either TLS and/or SRTP. Each application installed on the Computing Device must be selected from the CSfC Components List. The CSfC Components List provides several sections for which customers can select the TLS Application including Web Browser, Email Client, and VoIP Application. Physical separation between encryption components provides a number of security advantages, but also is more difficult to implement due to the required hardware users require.

For TLS EUDs, each application installed on the Computing Device is responsible for terminating the Inner Layer of Encryption. When a TLS EUD is composed of more than a single computing device, the Outer VPN Component is provided by an Outer VPN Gateway as shown in Figure D-4.

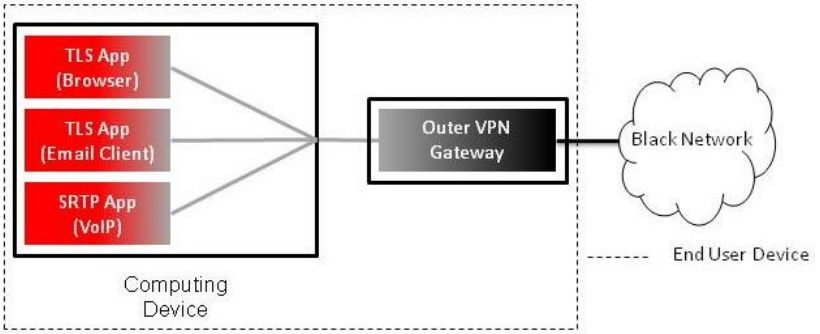

Figure D-4. TLS EUD with Separate Outer VPN Gateway

An Outer VPN client can be installed within the same computing device as the TLS Applications which provide the Inner Layer of Encryption as shown in Figure D-5. A retransmission device will also be required in this case, unless, as noted in Section 4.1.3, the connection is to a Wired Network, Domestic Cellular Network, Government Private Wireless Network or a Government Private Cellular network. See Figure D-6.

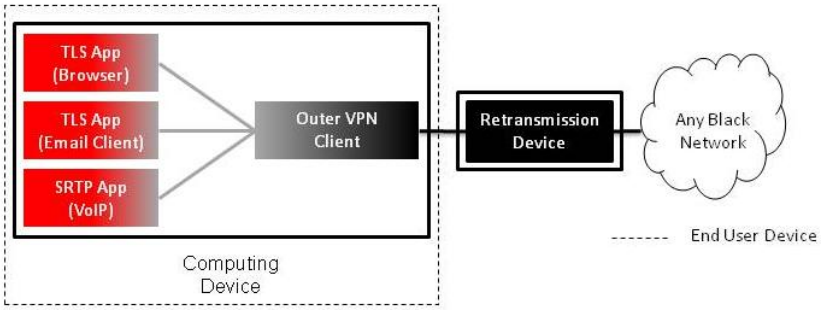

Figure D-5. TLS EUD with Integrated Outer VPN Client with Retransmission Device

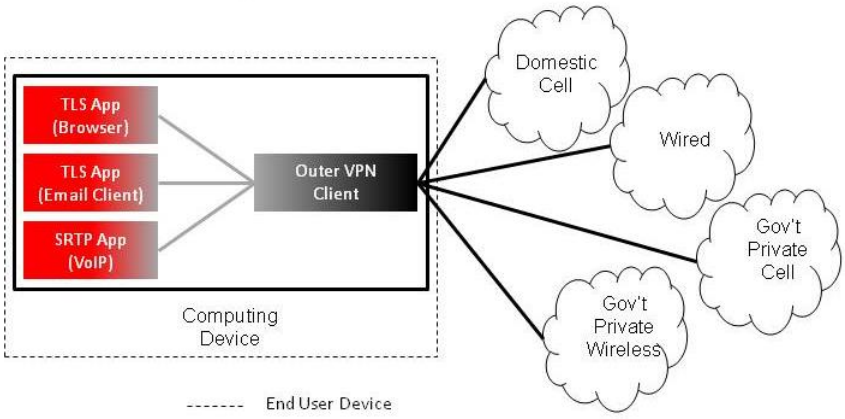

Figure D-6. TLS EUD with Integrated Outer VPN Client without Retransmission Device

Retransmission Devices:

A Government-owned Retransmission Device (RD) includes Wi-Fi Hotspots and Mobile Routers. On the external side, the RD can be connected to any type of medium (e.g. Cellular, Wi-Fi, SATCOM, Ethernet)

to gain access to the Wide Area Network. On the internal side the RD is connected to EUDs either through an Ethernet cable or Wi-Fi. See Figure D-7.

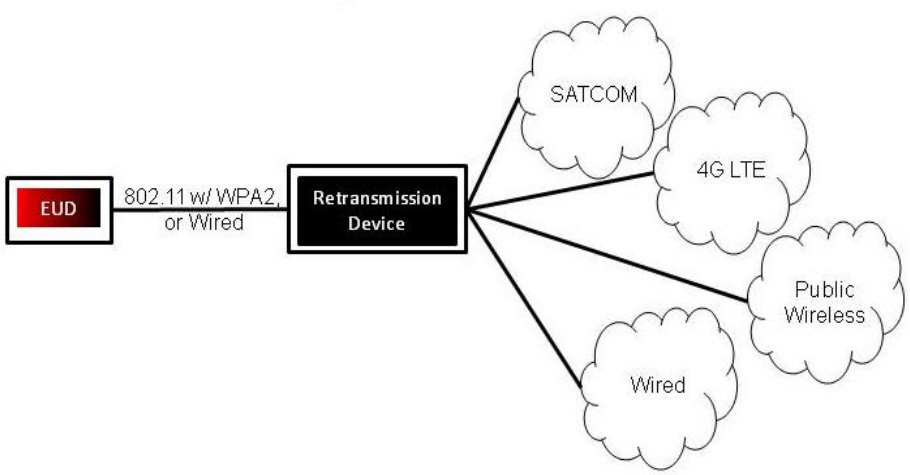

Figure D-7. Retransmission Device Connectivity

Solution Infrastructure supporting VPN and TLS EUDs

When supporting both VPN EUDs and TLS EUDs, the solution infrastructure will always include an Inner VPN Gateway between the Gray Firewall and Inner Firewall (data flow 1 in Figure D-8). Additionally, the solution infrastructure will include one or more TLS-Protected Servers. The TLS-Protected Servers are either placed between the Gray Firewall and Inner Firewall (data flow 2 in Figure D-8) or on the internal side of the Inner Firewall (data flow 3 in Figure D-8). Solutions including TLS-Protected Server(s) in the Enterprise/Red Network, TLS-Protected Server(s) between the Gray Firewall and Inner Firewall, and an Inner VPN Gateway will have at least three distinct data flows. Each Inner Encryption Components is independent and parallel to other Inner Encryption Components.

Figure X below, depicts a Mobile Access Solution which supports both TLS EUDs and VPN EUDs. While not required, the example below shows an example of implementing the TLS-Protected Servers both between the Gray Firewall and Inner Firewall and in the Enterprise/Red network.

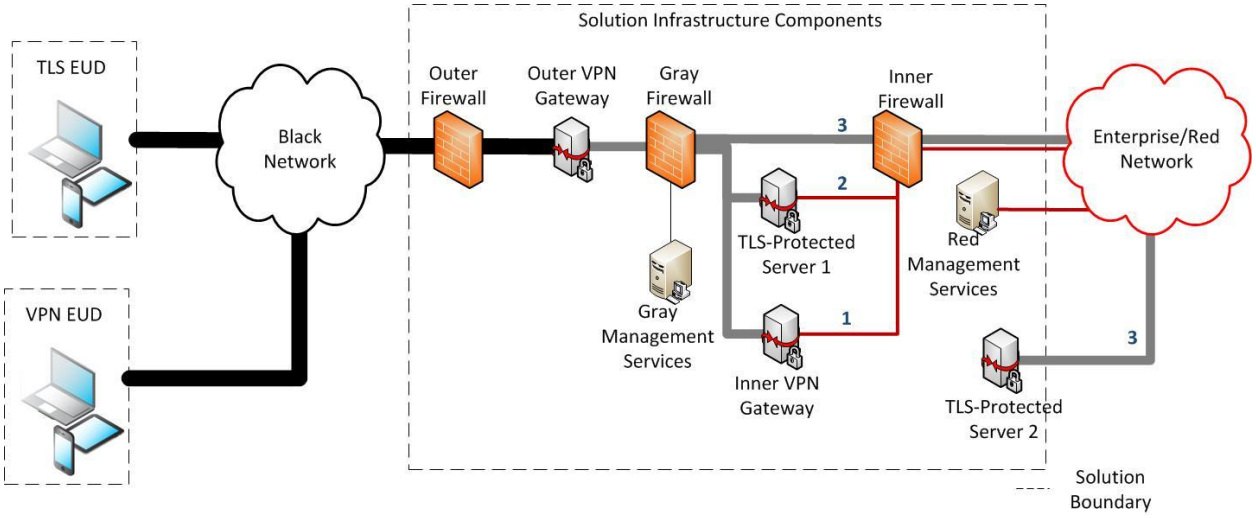

Figure D-8. Mobile Access Solution Infrastructure Supporting VPN and TLS EUDs

The following text describes each of the data flows depicted above.

1. The VPN Gateway terminates the Inner layer of IPSec traffic for all VPN EUDs, and authenticates the EUD VPN client based on device certificates. There is a physical connection between the Gray Firewall and the VPN Gateway and between the VPN Gateway and the Inner Firewall.
2. The TLS-Protected Server is placed between Gray Firewall and Inner Firewall. The TLS-Protected Server terminates the Inner layer of TLS traffic for one or more of the services available to TLS EUDs. The TLS-Protected Server could also be a Session Border Controller which terminates SRTP traffic and relays it to the appropriate destination in the Enterprise/Red network. The TLS-Protected Server authenticates the EUD's TLS client based on user or device certificates. There is a physical connection between the Gray Firewall and the TLS-Protected Server and between the TLS-Protected Server and the Inner Firewall. This connection is in parallel with the VPN Gateway such that the TLS-Protected server is not dependent on the Inner-VPN Gateway to reach the Gray Firewall or the Inner Firewall.
3. When a TLS-Protected Server is placed within the Enterprise/Red network, it is still considered part of the Mobile Access Solution. The TLS-Protected Server terminates the Inner layer of TLS traffic for one or more of the services available to TLS EUDs. The TLS-Protected Server depicted could also be a SRTP Endpoint which terminates SRTP traffic for real-time voice and video services. When the TLS-Protected Server is located in the Enterprise/Red network, there is a direct physical connection between the Gray Firewall and Inner Firewalls. This connection is in parallel with the VPN Gateway such that traffic destined for the TLS-Protected Server is not dependent on the Inner VPN Gateway or any other TLS-Protected Server to reach the Gray Firewall or the Inner Firewall. The Gray Firewall and Inner Firewalls shall be configured with an ACL to only permit traffic to TLS-Protected Servers in the Enterprise/Red network with appropriate source/destination IP addresses and ports.

APPENDIX E. TACTICAL SOLUTION IMPLEMENTATIONS

Although the majority of customers instantiating solutions based on the Mobile Access CP will be utilized for Strategic or Operational Environments, some organizations may deploy the MA CP in Tactical environments. These Tactical Environments include a specific set of Size, Weight, and Power (SWaP) constraints not found in traditional environments.

Organizations intending to deploy an MA CP Solution for Tactical Environments may utilize this Appendix which accommodates the SWaP constraints unique to their environment. This Appendix may only be utilized to protect Tactical Data classified as SECRET or below. The CP follows CNSSI 4009 which defines Tactical Data as "Information that requires protection from disclosure and modification for a limited duration as determined by the originator or information owner." In addition to protecting Tactical Data, organizations which register their solution using this Appendix must be deployed at the Tactical Edge. The CP also follows CNSSI 4009 which defines the Tactical Edge as "The platforms, sites, and personnel (U. S. military, allied, coalition partners, first responders) operating at lethal risk in a battle space or crisis environment characterized by 1) a dependence on information systems and connectivity for survival and mission success, 2) high threats to the operational readiness of both information systems and connectivity, and 3) users are fully engaged, highly stressed, and dependent on the availability, integrity, and transparency of their information systems."

If an organization's planned solution meets the two above criteria then their solution may be registered utilizing the requirement accommodations in this Appendix. The MA CP Registration form must explicitly state that the solution is being utilized in Tactical Environments and provide justification on how the above criteria are met. In general, customers registering with this Appendix will be deployed in support of Battalion and below (or equivalent) unit structure. Typically, these Tactical Environments are located in austere environments where communication infrastructure is generally limited. Due to the lack of existing communication infrastructure, the Tactical Environments are also generally characterized by the use of Government owned Black Infrastructure (Government Private Wireless Networks and/or Government Private Cellular Networks).

The below table may be utilized by customers meeting the above criteria when configuring, testing, registering, and operating their Mobile Access Solution. Any questions on the use of this Appendix should be directed to mobile_access@nsa.gov and csfc@nsa.gov.

Table 31. Tactical Implementation Requirements Overlay

Req #	Requirement Description	Capabilities	Threshold / Objective	Alternative
MA-PS-17	The Outer firewall, Outer VPN Gateway, Gray firewall, Inner Encryption Component, and Inner firewall shall use physically separate components, such that no component is used for more than one function (see Figure 1).	VI, TI	O	MA-TO-1
MA-TO-1	The Outer VPN Gateway shall be physically separate from the Inner Encryption Components	VI, TI	T	MA-PS-17
MA-EU-12	Users of EUDs shall successfully authenticate themselves to the services they access on the Red network using an AO approved method.	VE, TE	O	
MA-EU-13	Red network services shall not transmit any classified data to EUDs until user authentication succeeds.	VE, TE	O	
MA-MR-5	Each IDS in the solution shall be configured to send alerts to the Security Administrator.	All	O	
MA-MR-7	The organization shall create IDS rules that generate alerts upon detection of any unauthorized destination IP addresses.	All	O	
MA-DM-14	The Outer VPN Gateway and solution components within the Gray network shall forward log entries to a SIEM on the Gray Management network (or SIEM in the Enterprise/Red Network if using an AO approved one-way tap) within 10 minutes.	VI, TI	O	